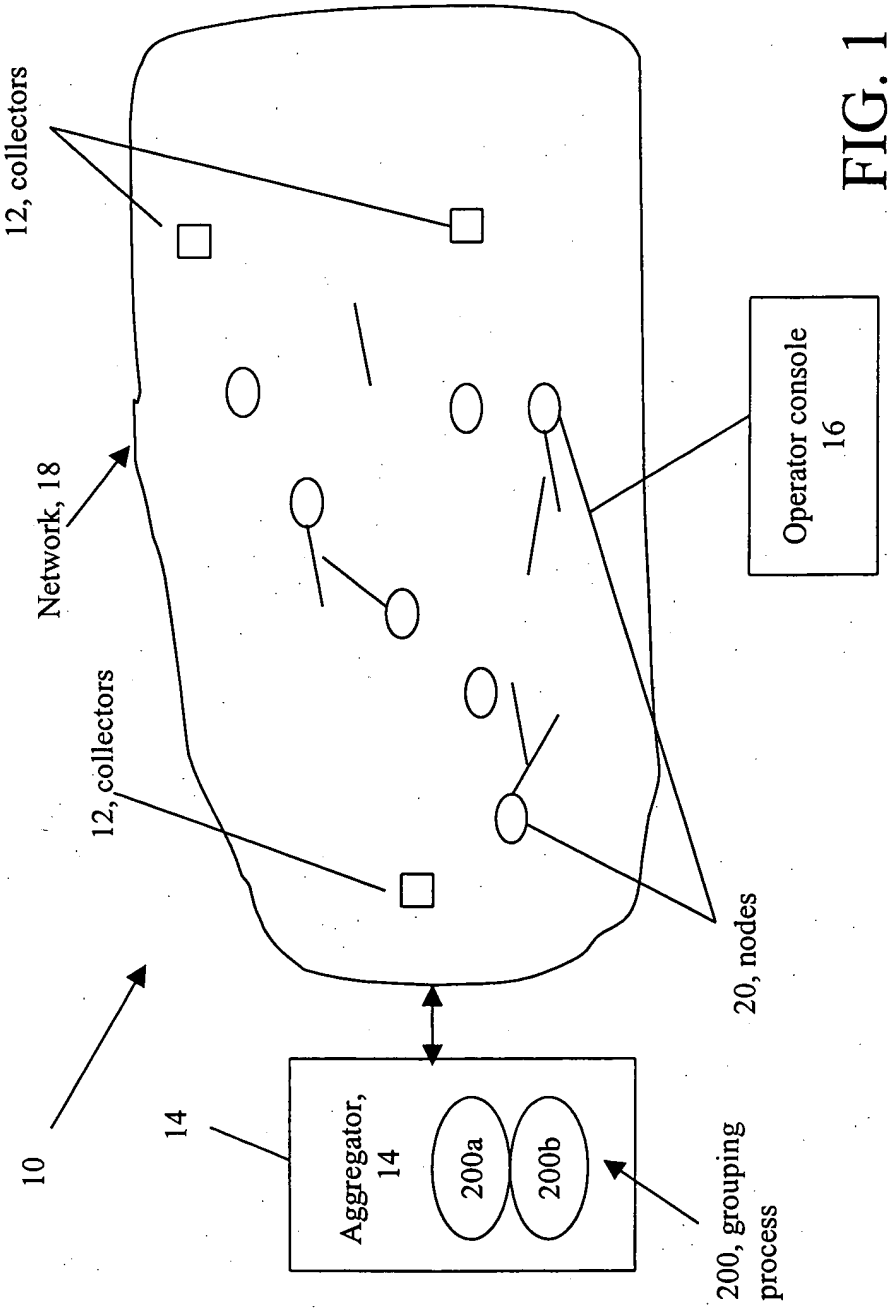

12, collectors
Network, 18
Operator console
16
12, collectors
20, nodes
10
14
Aggregator,
14
200a
200b
200, grouping
process

FIG. 1

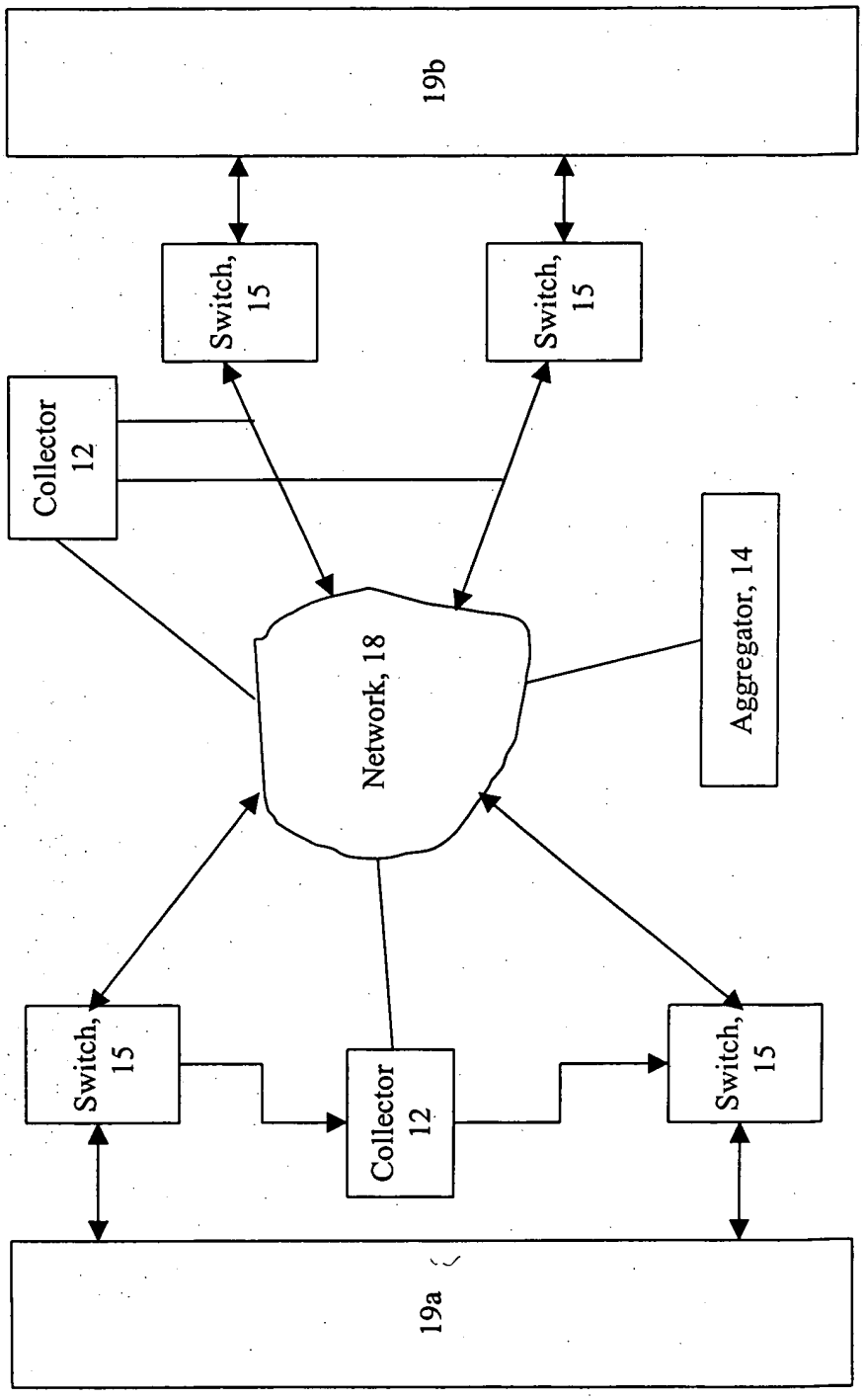

19b
Switch, 15
Switch, 15
15b
Collector 12
Aggregator, 14
Network, 18
Switch, 15
Collector 12
Switch, 15
15a
19a

FIG. 2

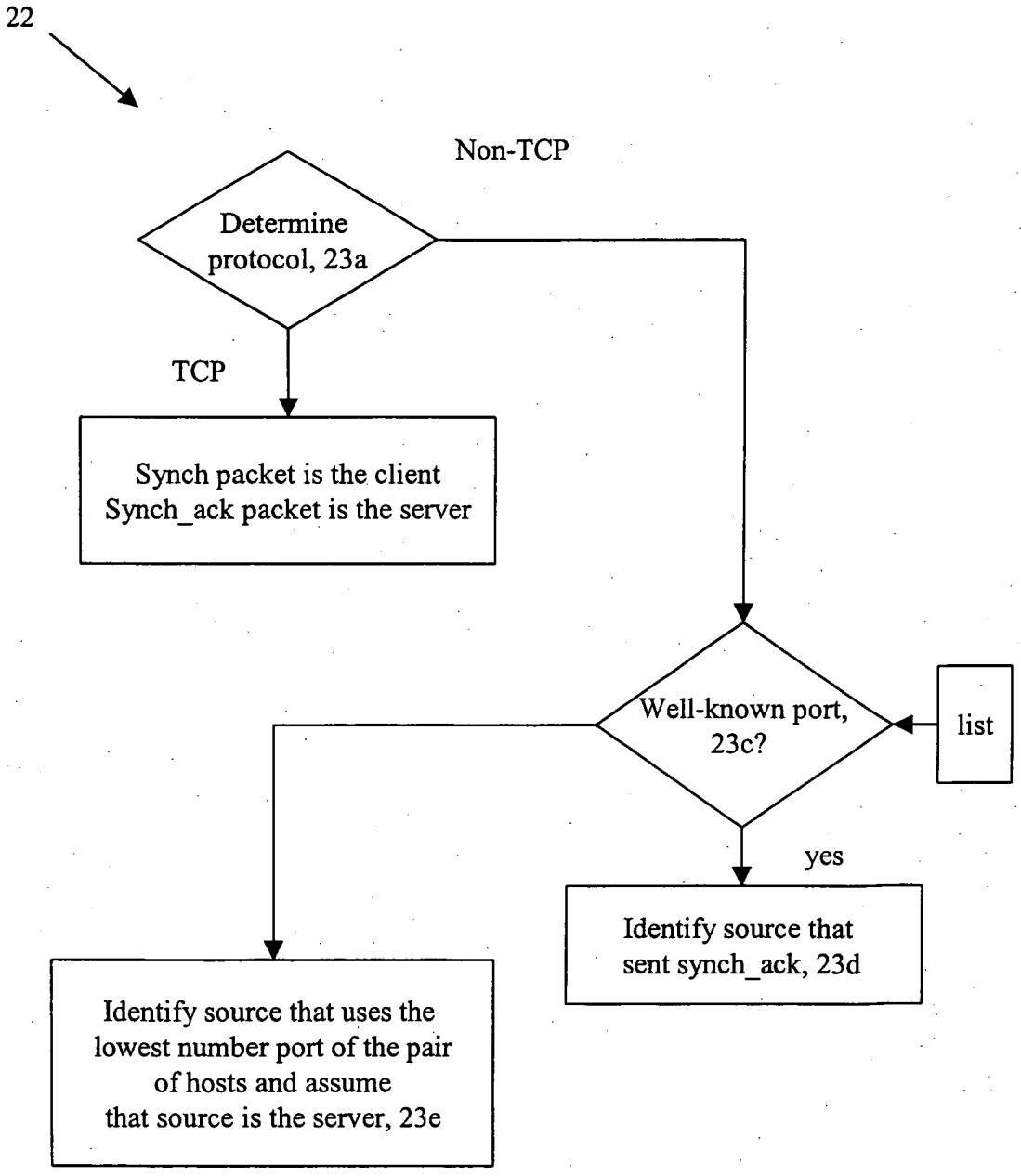

22
Non-TCP
Determine protocol, 23a
TCP
Synch packet is the client Synch_ack packet is the server
Well-known port, 23c?
list
yes
Identify source that sent synch_ack, 23d
Identify source that uses the lowest number port of the pair of hosts and assume that source is the server, 23e

FIG. 2A

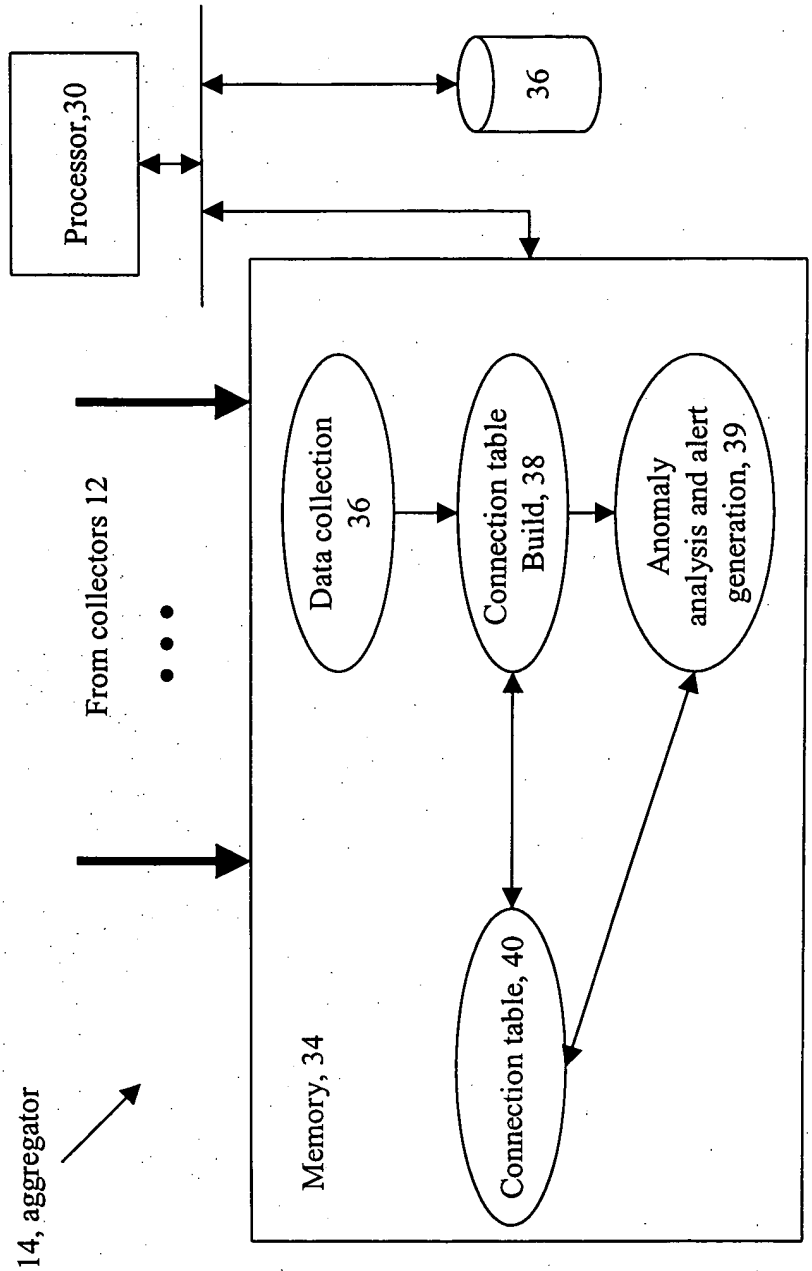

Processor,30
36
From collectors 12
Data collection
36
Connection table
Build, 38
Anomaly
analysis and alert
generation, 39
Memory, 34
Connection table, 40
14, aggregator

FIG. 3

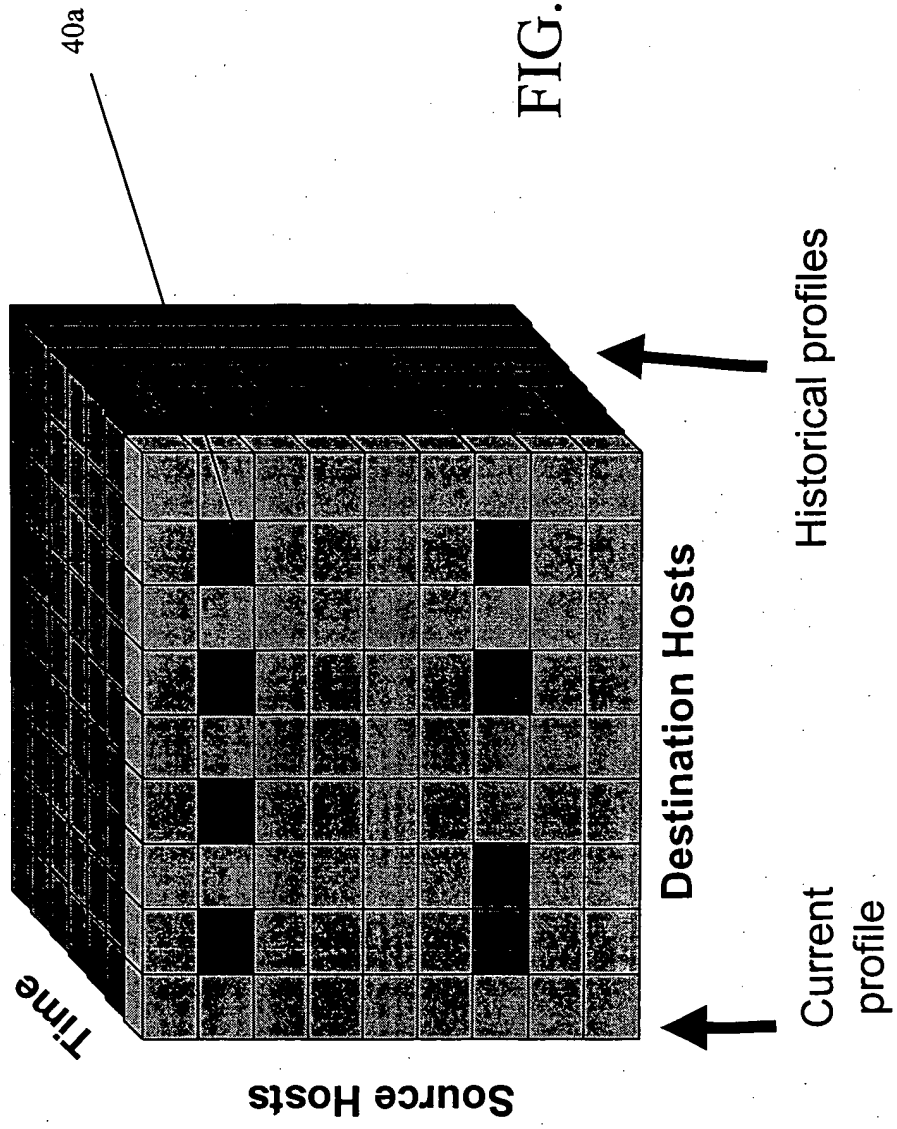

40a
Historical profiles
Destination Hosts
Current profile
Time
Source Hosts

FIG. 4

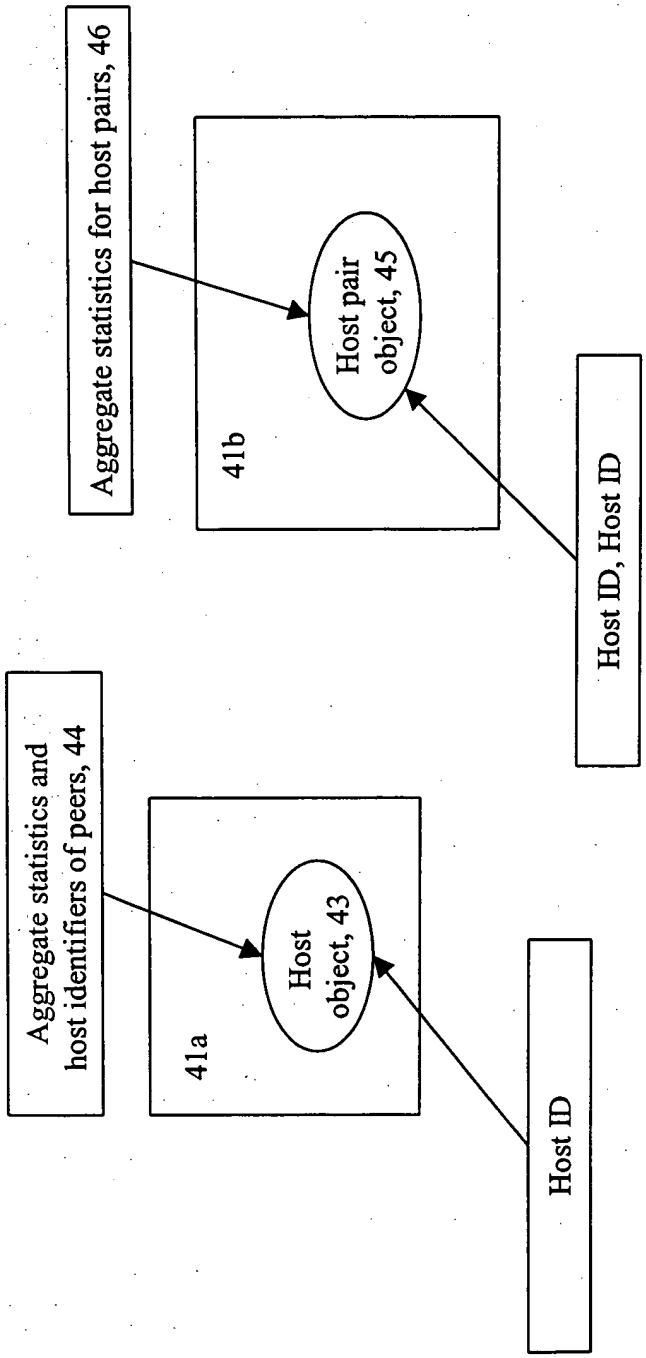

Aggregate statistics for host pairs, 46
41b
Host pair object, 45
Host ID, Host ID
Aggregate statistics and host identifiers of peers, 44
41a
Host object, 43
Host ID
Group Information, 47

FIG. 4A

Time Slice	**Fri**	Thu	Wed	…	Sun	Sat	Fri
Services provided by A (Web Server) to B (Desktop)							
WWW (TCP:80)							
Bytes / sec	**2k**	**3k**	**1k**	**…**	**2k**	**4k**	**3k**
Packets / sec	**5**	**6**	**2**		**5**	**9**	**5**
Conn's. / hr	**.3**	**.5**	**.3**		**.2**	**.3**	**.3**
SSH (TCP:22)							
Bytes / sec	**1k**	**3k**	**4k**	**…**	**1k**	**2k**	**3k**
Packets / sec	**2**	**6**	**9**		**2**	**5**	**6**
Conn's. / hr	**.3**	**.5**	**.3**		**.3**	**.3**	**.5**
				…			
Services provided by B (Desktop) to A (Web Server)							
SSH (TCP:22)							
Bytes / sec	**21k**	**0**	**0**	**…**	**0**	**0**	**0**
Packets / sec	**10**	**0**	**0**		**0**	**0**	**0**
Conn's. / hr	**1**	**0**	**0**		**0**	**0**	**0**

FIG. 5

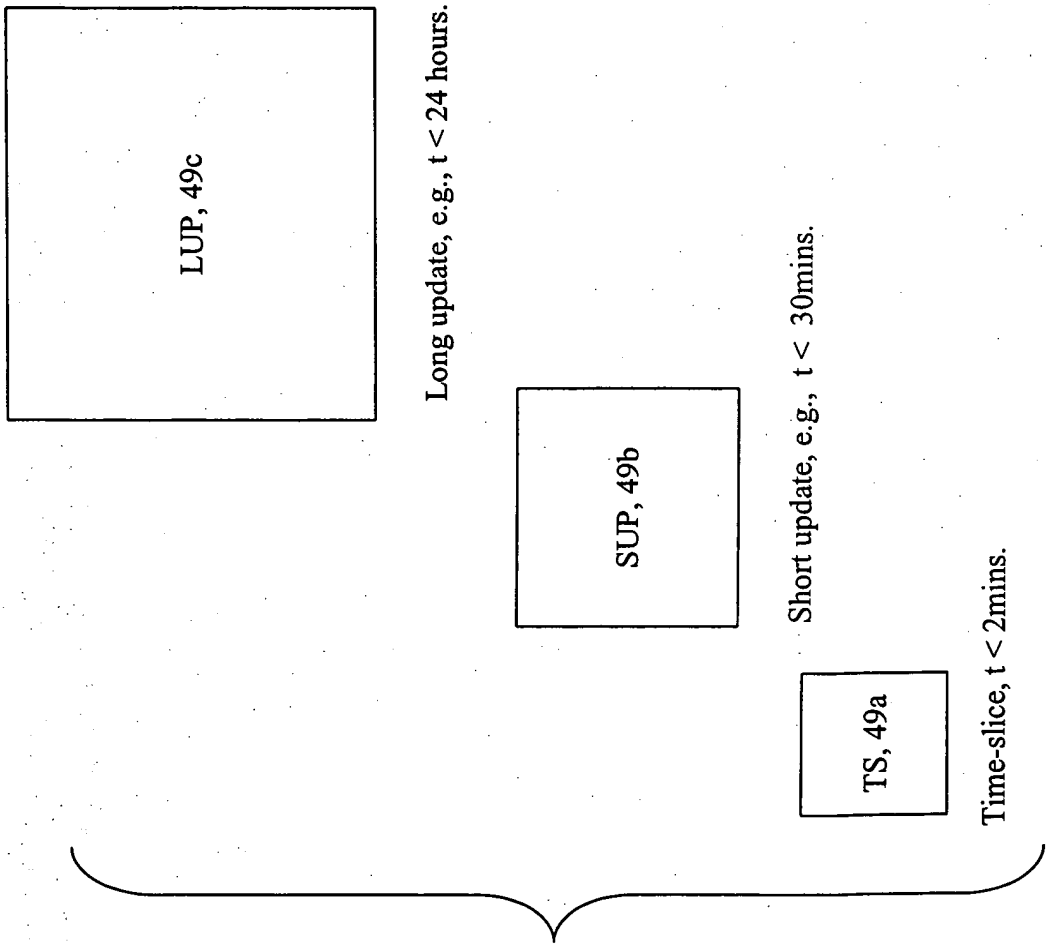

LUP, 49c
Long update, e.g., t < 24 hours.
SUP, 49b
Short update, e.g., t < 30mins.
TS, 49a
Time-slice, t < 2mins.
40

FIG. 6

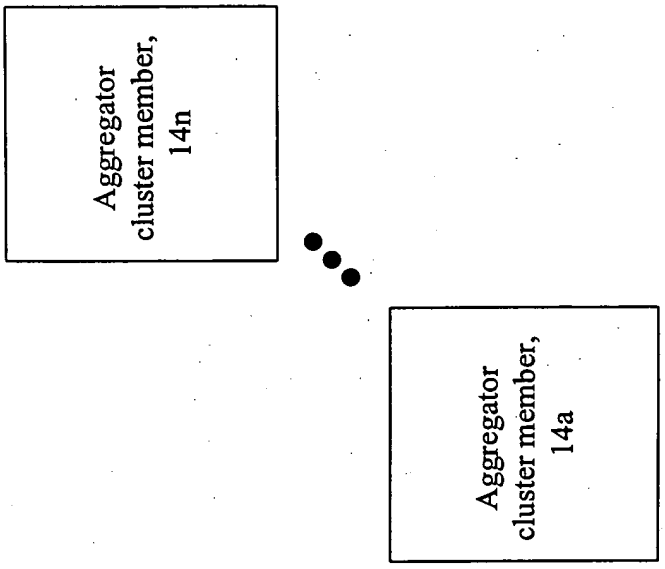
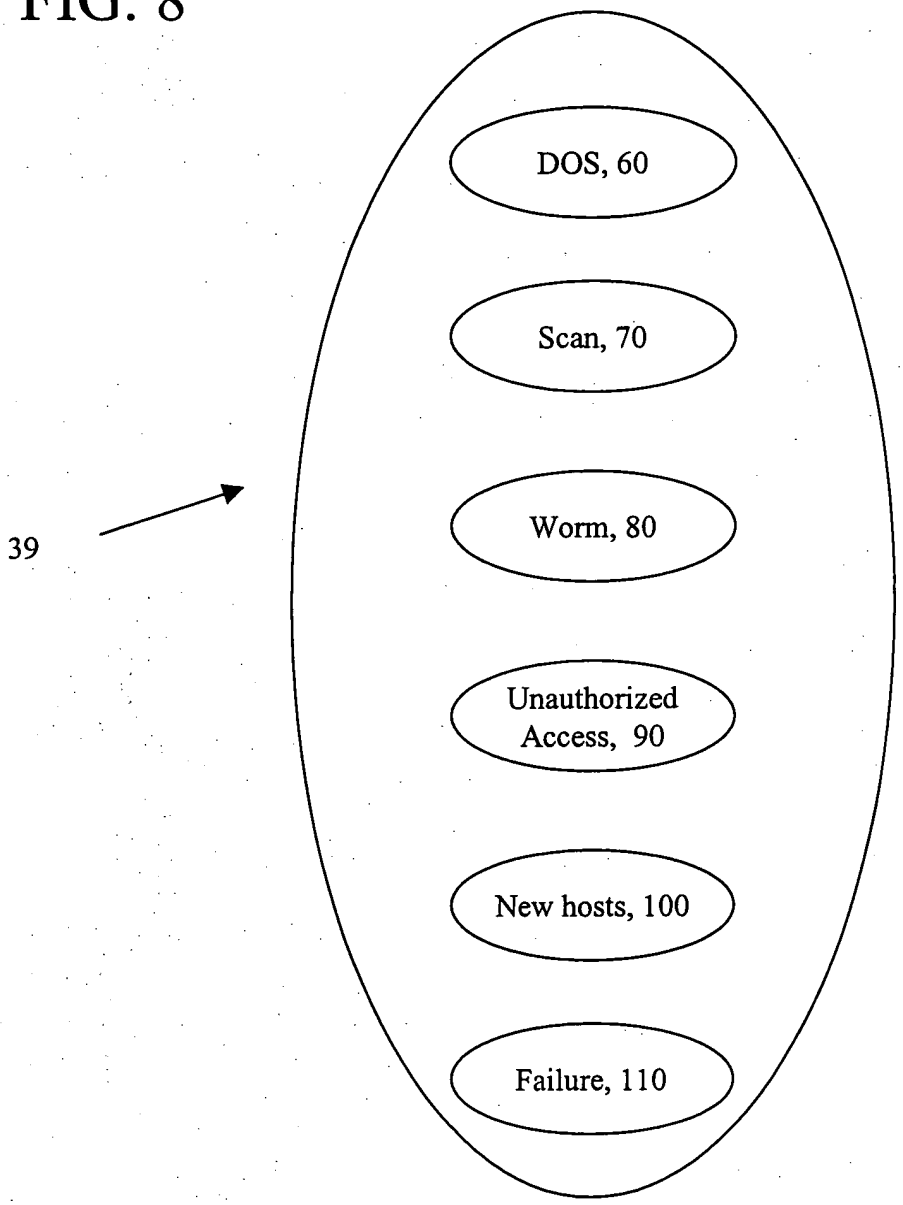

Aggregator cluster member, 14n
Aggregator cluster member, 14a

FIG. 7

FIG. 8


39
DOS, 60
Scan, 70
Worm, 80
Unauthorized Access, 90
New hosts, 100
Failure, 110

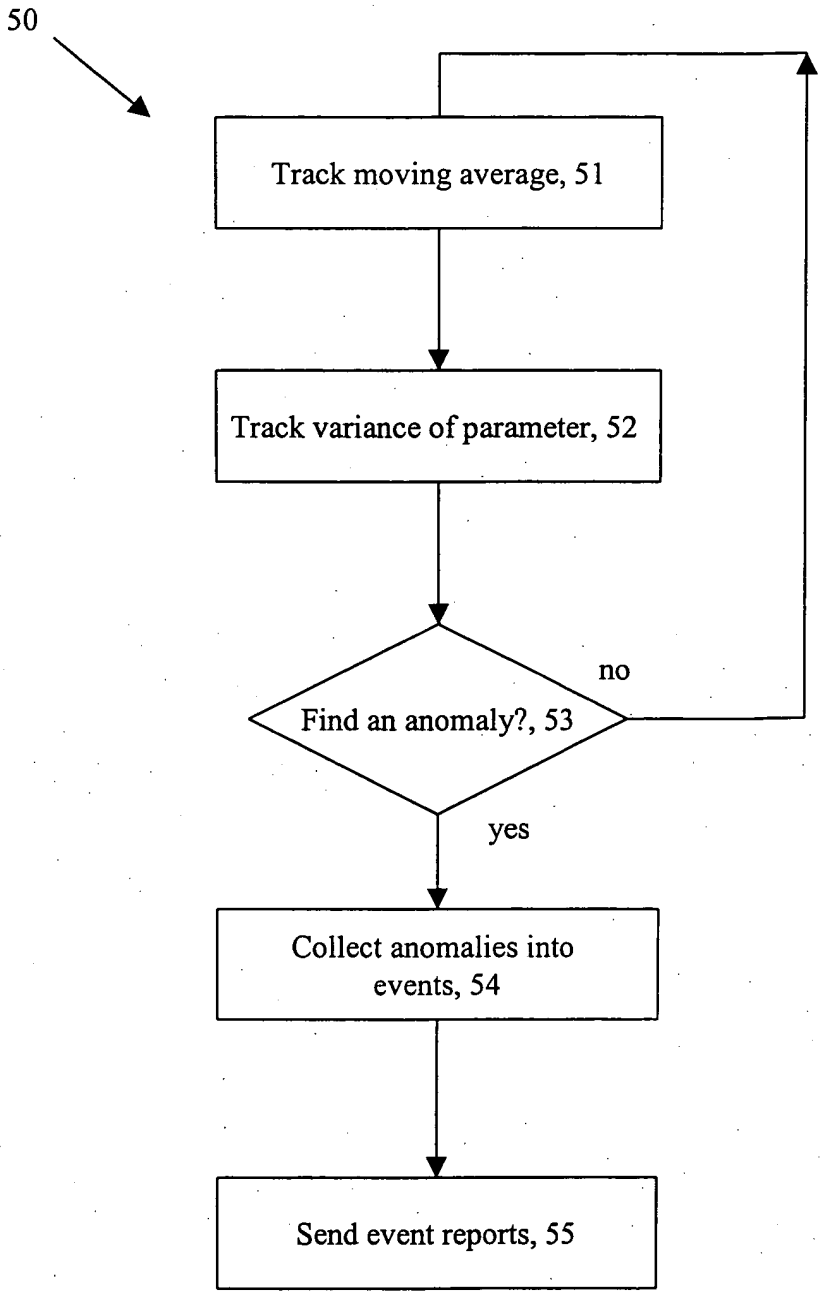

50
Track moving average, 51
Track variance of parameter, 52
Find an anomaly?, 53
no
yes
Collect anomalies into events, 54
Send event reports, 55

FIG. 9

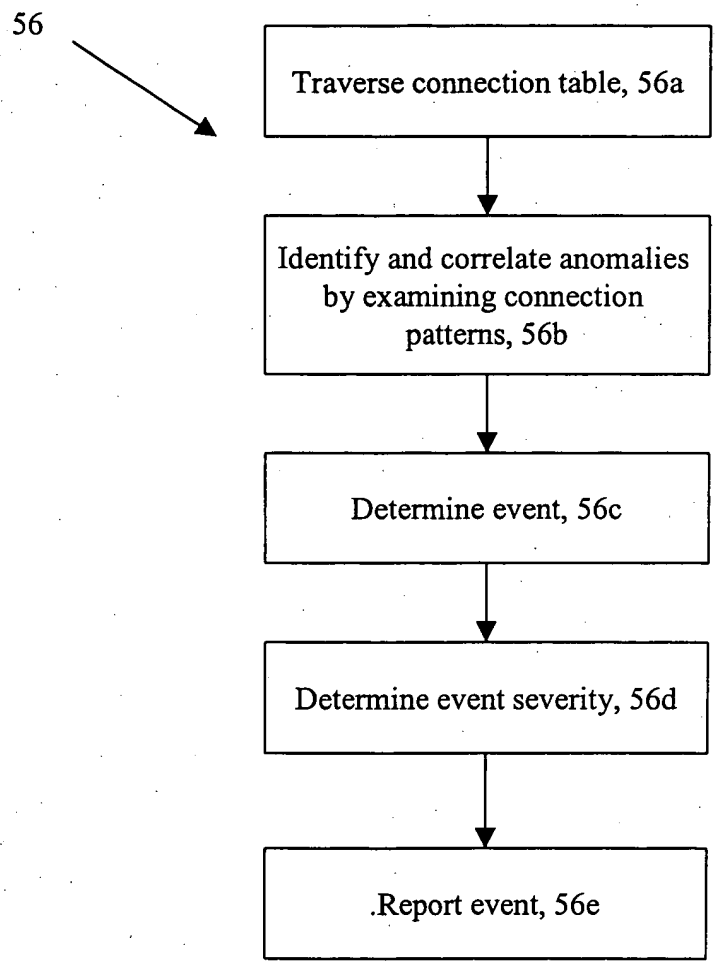

56
Traverse connection table, 56a
Identify and correlate anomalies by examining connection patterns, 56b
Determine event, 56c
Determine event severity, 56d
.Report event, 56e

FIG. 10

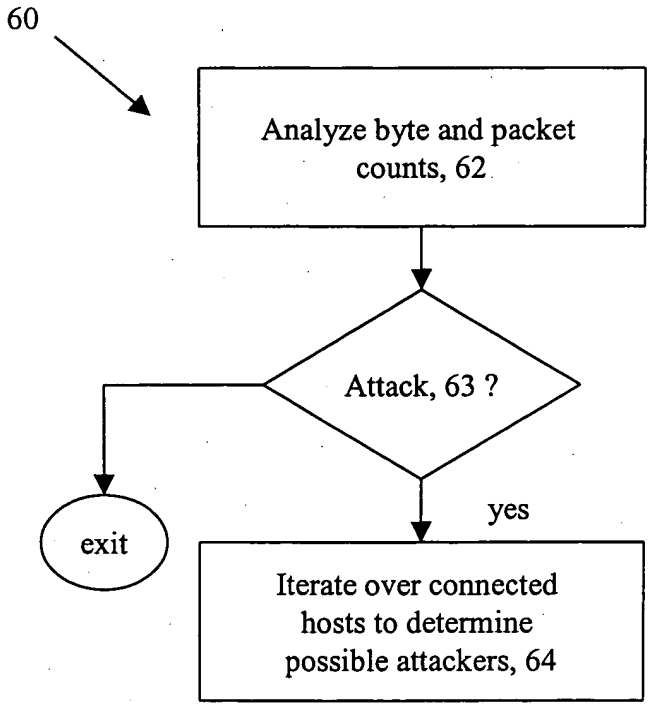

60
Analyze byte and packet counts, 62
Attack, 63 ?
yes
exit
Iterate over connected hosts to determine possible attackers, 64

FIG. 11

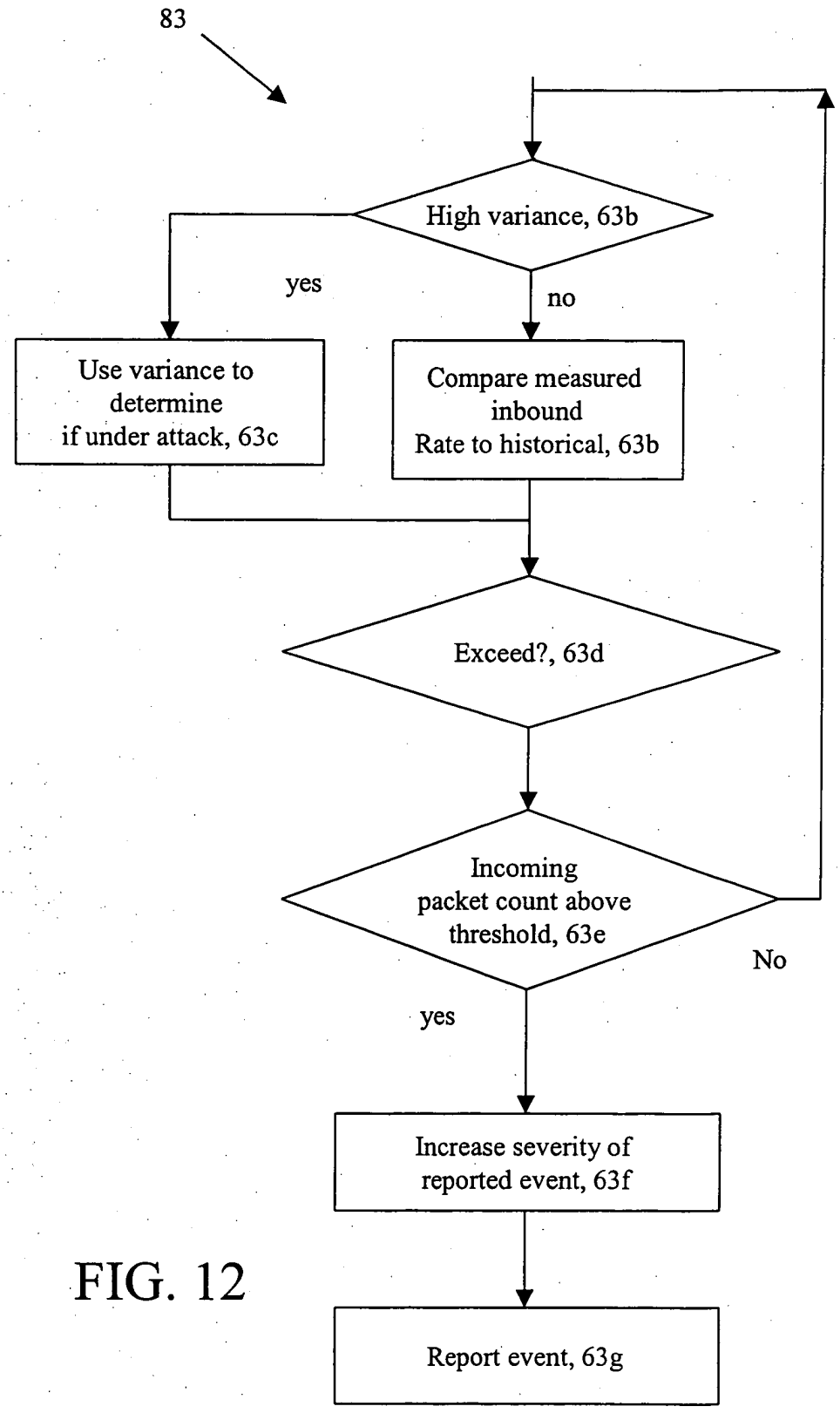

83
High variance, 63b
yes
no
Use variance to determine if under attack, 63c
Compare measured inbound Rate to historical, 63b
Exceed?, 63d
Incoming packet count above threshold, 63e
No
yes
Increase severity of reported event, 63f
Report event, 63g

FIG. 12

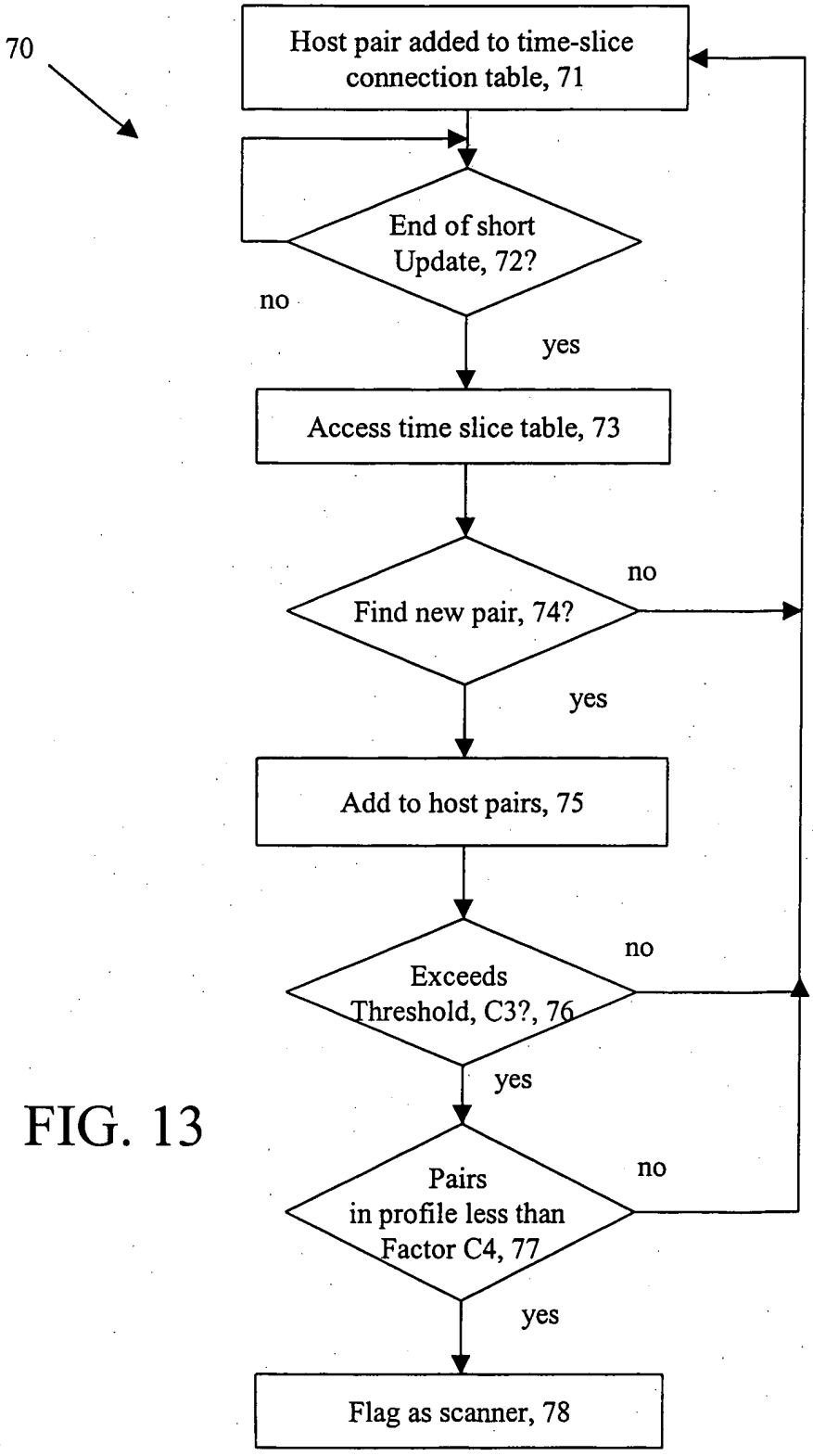

70
Host pair added to time-slice connection table, 71
End of short Update, 72?
no
yes
Access time slice table, 73
Find new pair, 74?
no
yes
Add to host pairs, 75
Exceeds Threshold, C3?, 76
no
yes
Pairs in profile less than Factor C4, 77
no
yes
Flag as scanner, 78

FIG. 13

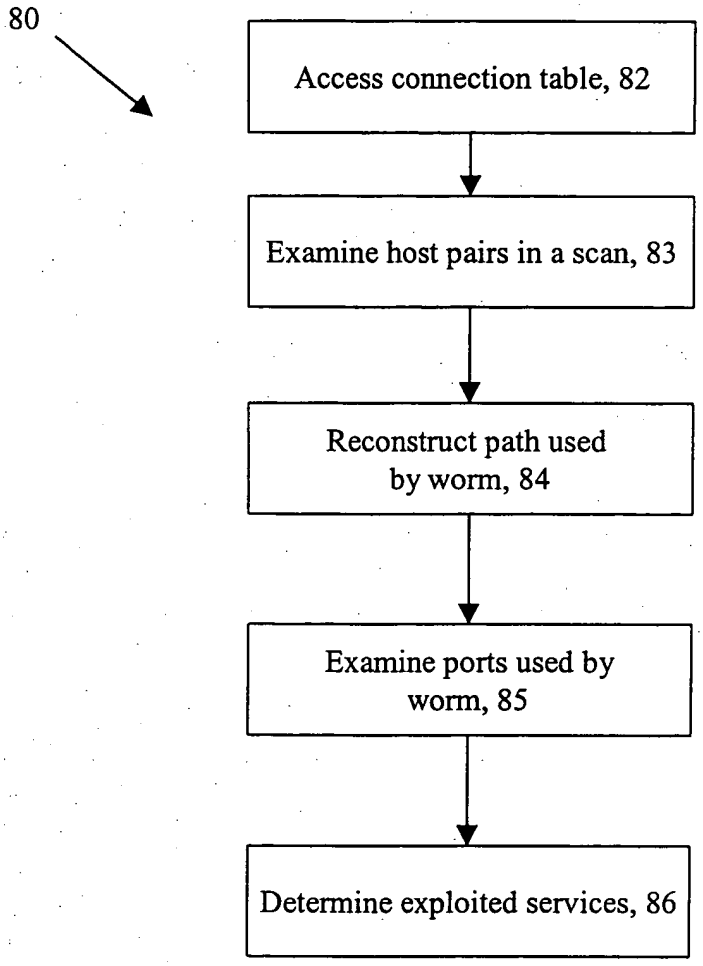

80
Access connection table, 82
Examine host pairs in a scan, 83
Reconstruct path used by worm, 84
Examine ports used by worm, 85
Determine exploited services, 86

FIG. 14

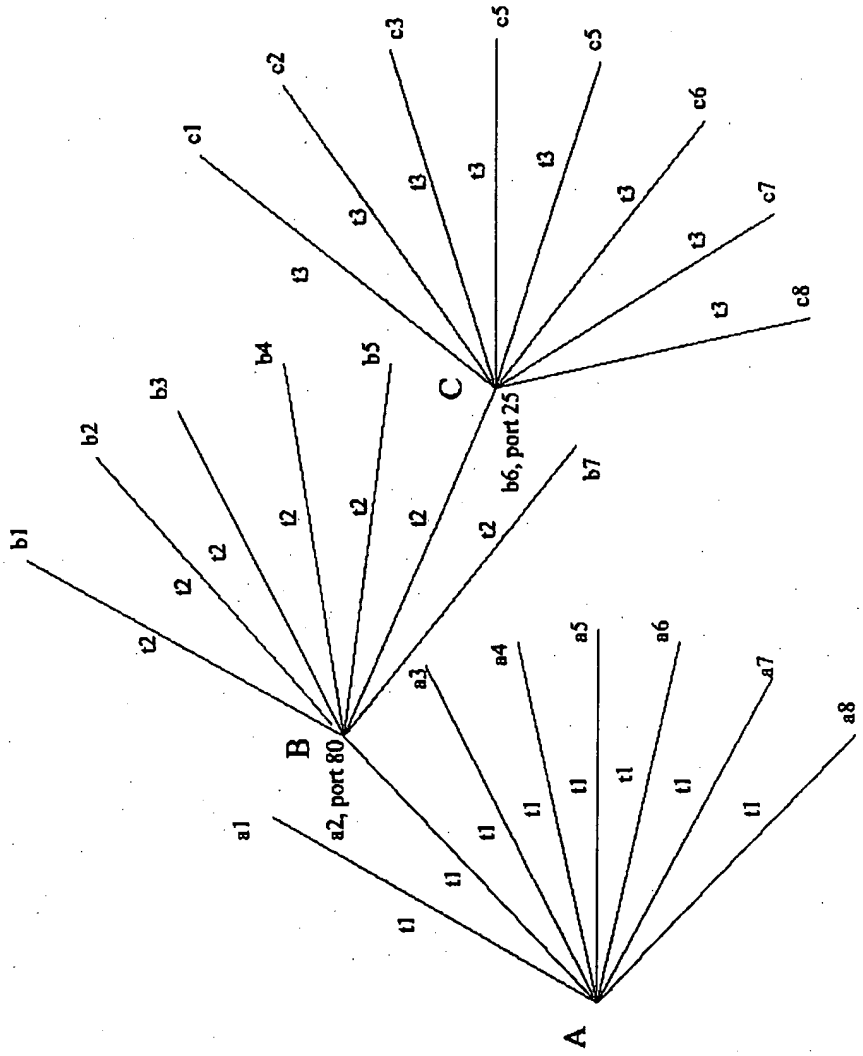

A
B
a2, port 80
C
b6, port 25
a1
a2
a3
a4
a5
a6
a7
a8
b1
b2
b3
b4
b5
b7
c1
c2
c3
c5
c5
c6
c7
c8
t1
t2
t3

FIG. 15

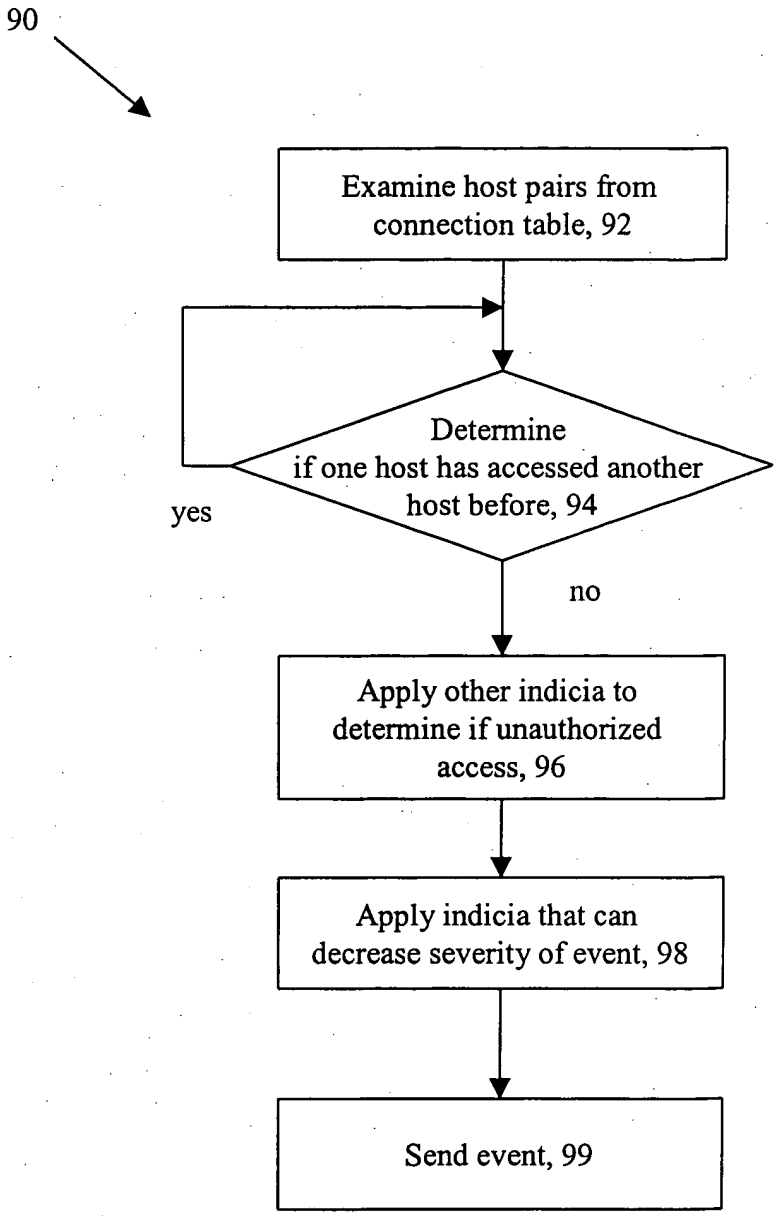

90
Examine host pairs from connection table, 92
Determine if one host has accessed another host before, 94
yes
no
Apply other indicia to determine if unauthorized access, 96
Apply indicia that can decrease severity of event, 98
Send event, 99

FIG. 16

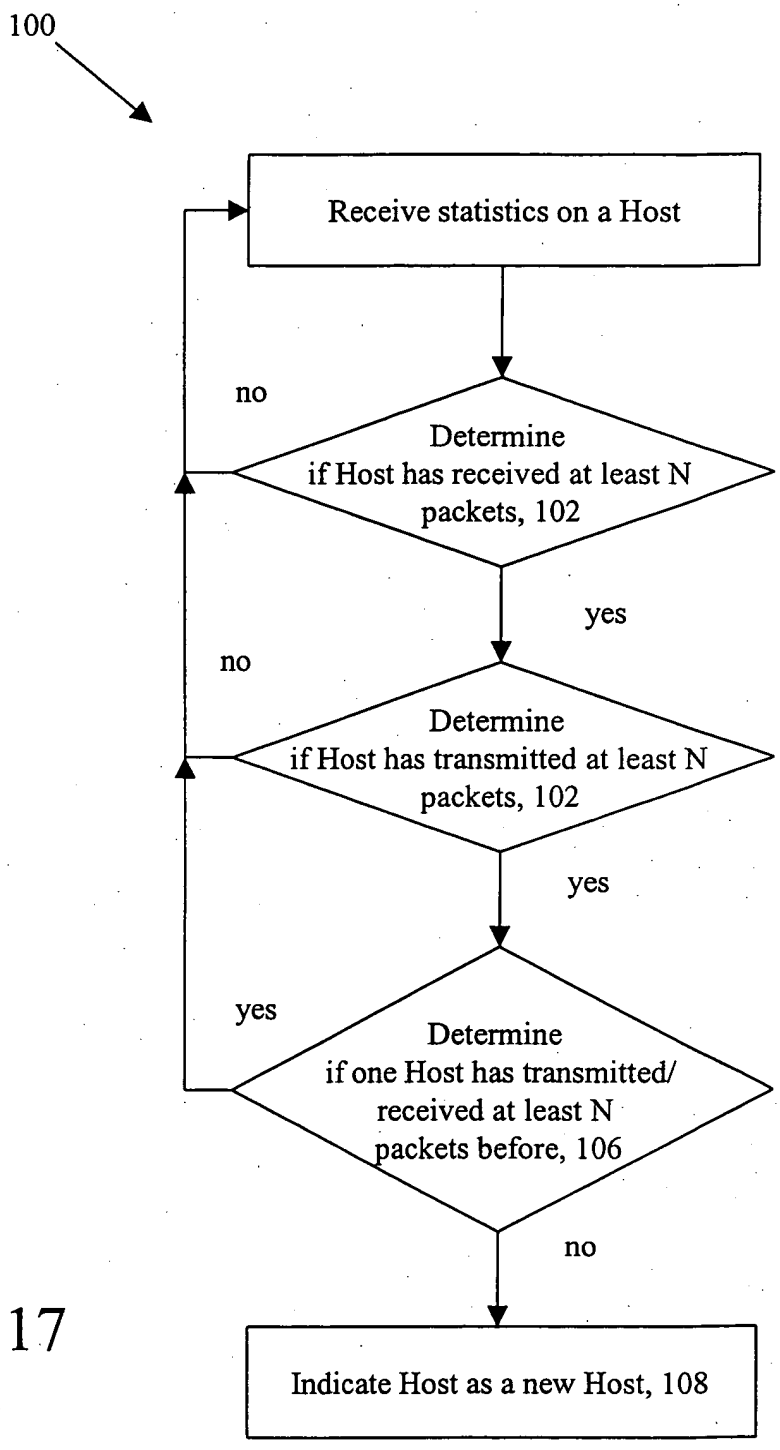

100
Receive statistics on a Host
Determine if Host has received at least N packets, 102
no
yes
Determine if Host has transmitted at least N packets, 102
no
yes
Determine if one Host has transmitted/ received at least N packets before, 106
yes
no
Indicate Host as a new Host, 108

FIG. 17

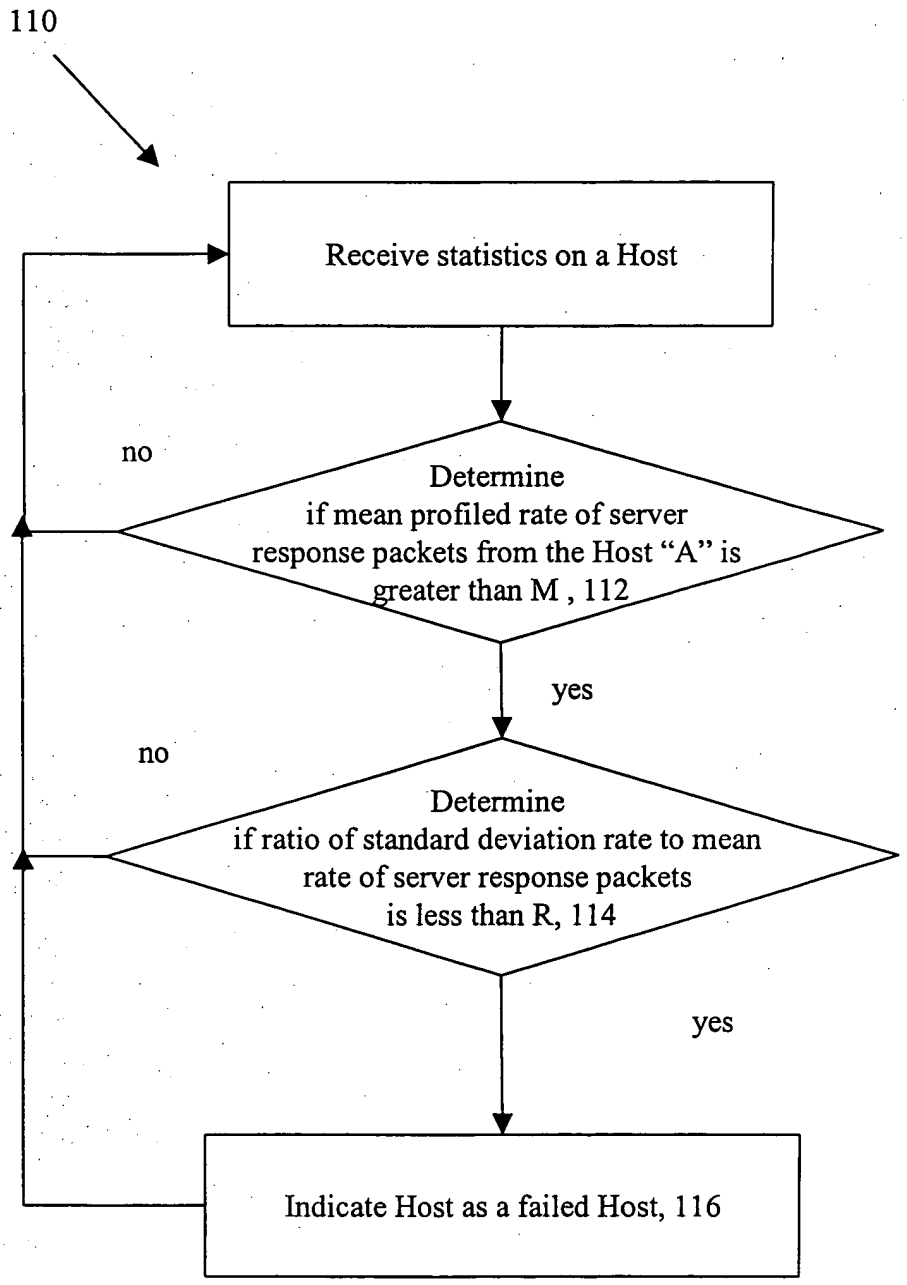

110
Receive statistics on a Host
no
Determine
if mean profiled rate of server
response packets from the Host "A" is
greater than M , 112
yes
no
Determine
if ratio of standard deviation rate to mean
rate of server response packets
is less than R, 114
yes
Indicate Host as a failed Host, 116

FIG. 18

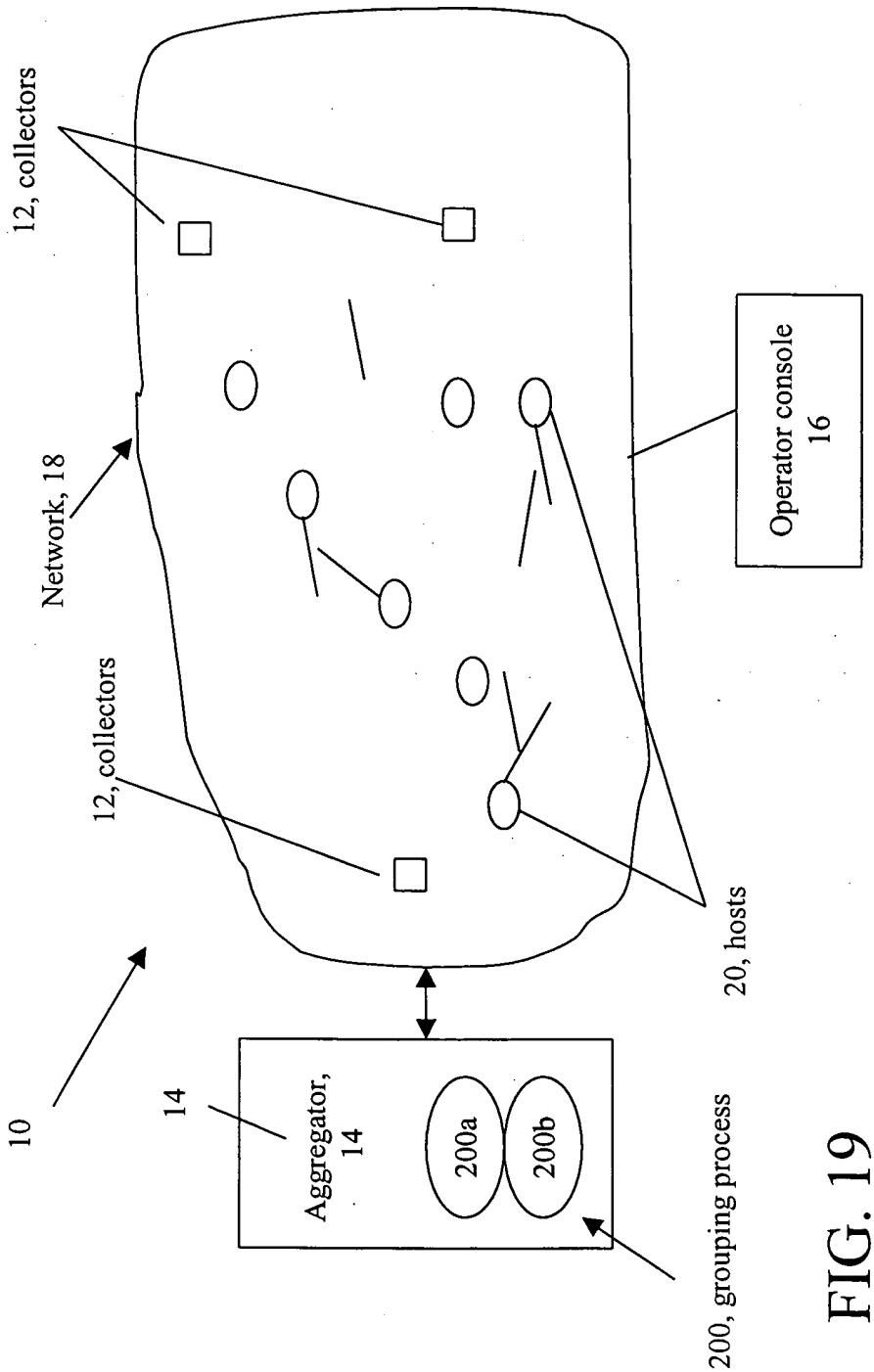

12, collectors
Network, 18
Operator console
16
12, collectors
20, hosts
10
14
Aggregator,
14
200a
200b
200, grouping process

FIG. 19

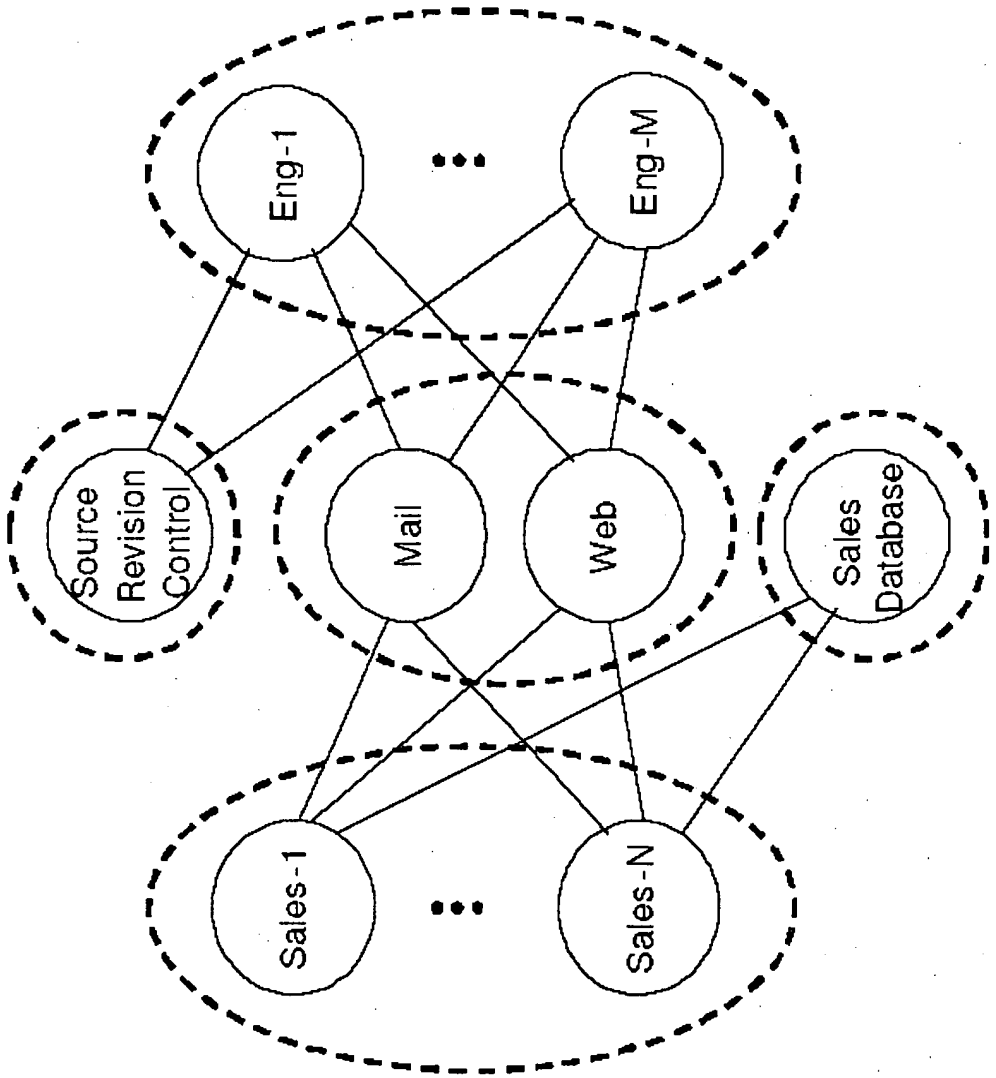

Eng-1
Eng-M
Source Revision Control
Mail
Web
Sales Database
Sales-1
Sales-N

FIG. 20

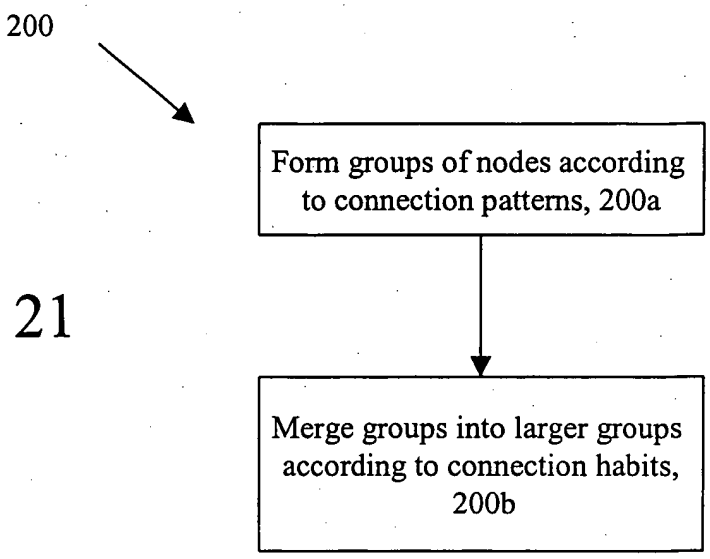

200
Form groups of nodes according to connection patterns, 200a
Merge groups into larger groups according to connection habits, 200b

FIG. 21

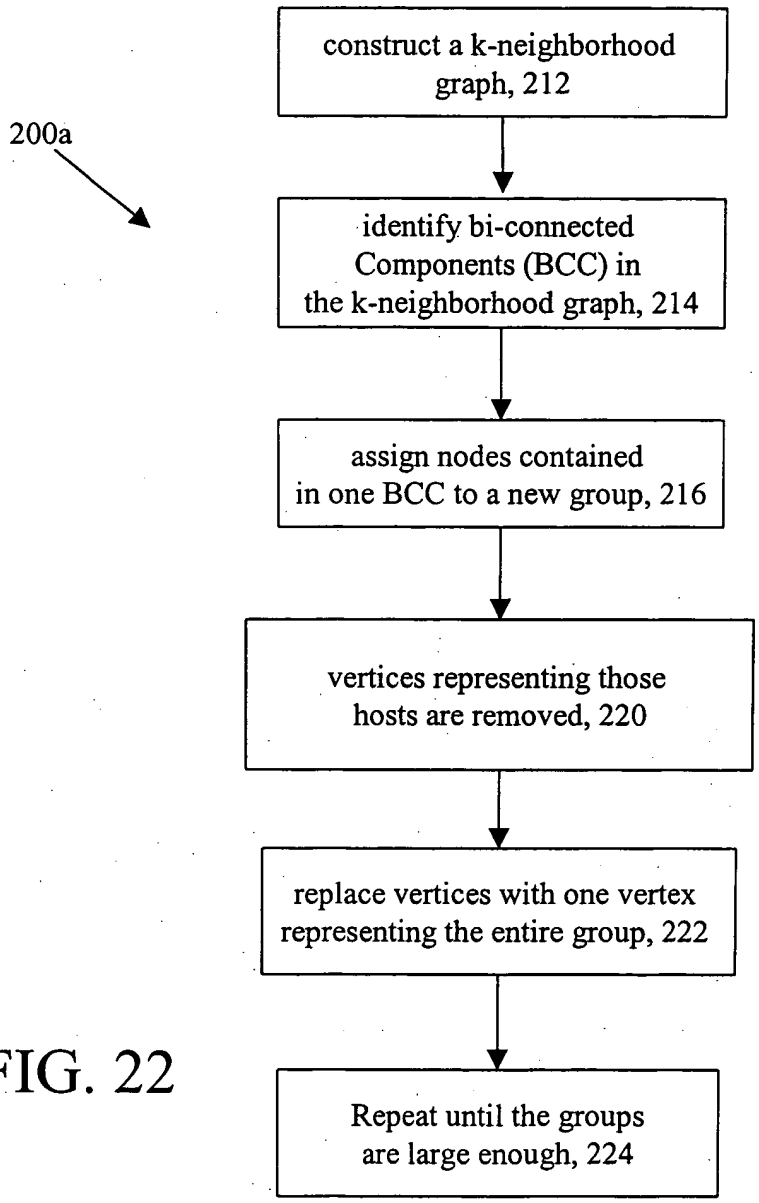

200a
construct a k-neighborhood graph, 212
identify bi-connected Components (BCC) in the k-neighborhood graph, 214
assign nodes contained in one BCC to a new group, 216
vertices representing those hosts are removed, 220
replace vertices with one vertex representing the entire group, 222
Repeat until the groups are large enough, 224

FIG. 22

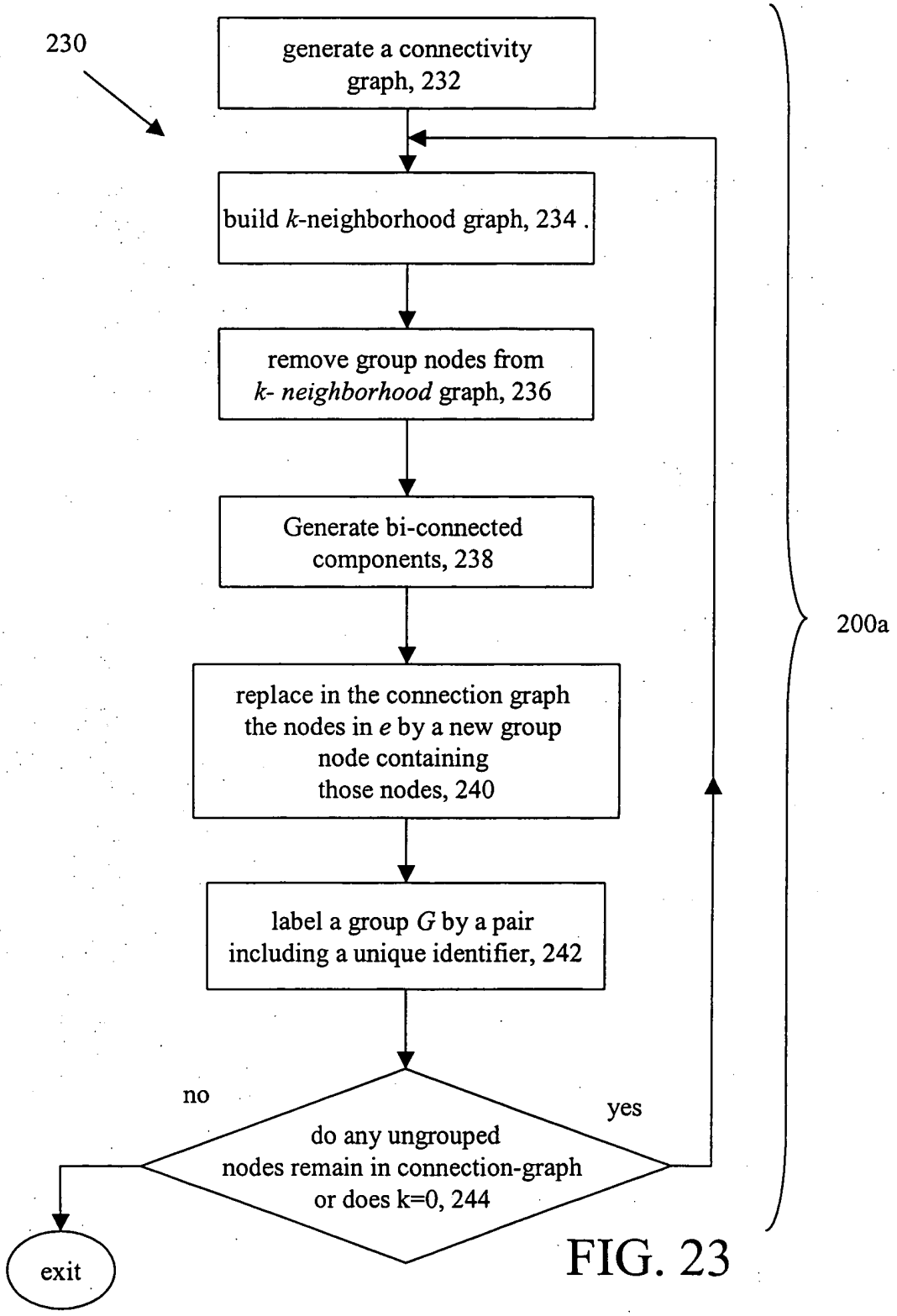

230
generate a connectivity graph, 232
build k-neighborhood graph, 234 .
remove group nodes from k- neighborhood graph, 236
Generate bi-connected components, 238
replace in the connection graph the nodes in e by a new group node containing those nodes, 240
label a group G by a pair including a unique identifier, 242
do any ungrouped nodes remain in connection-graph or does k=0, 244
no
yes
exit
200a

FIG. 23

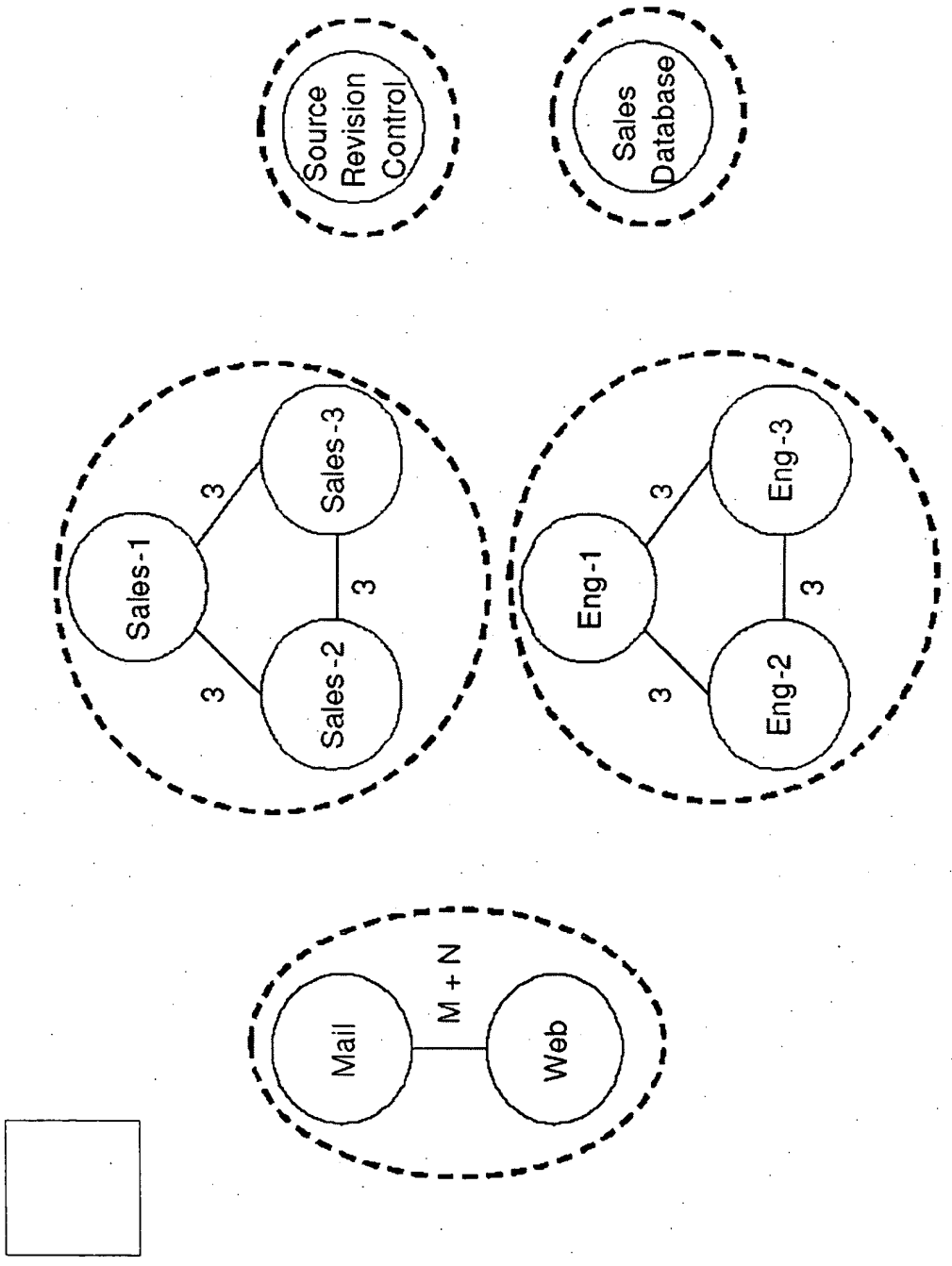

Source Revision Control
Sales Database
Sales-1
Sales-2
Sales-3
3
3
3
Eng-1
Eng-2
Eng-3
3
3
3
Mail
M + N
Web

FIG. 24

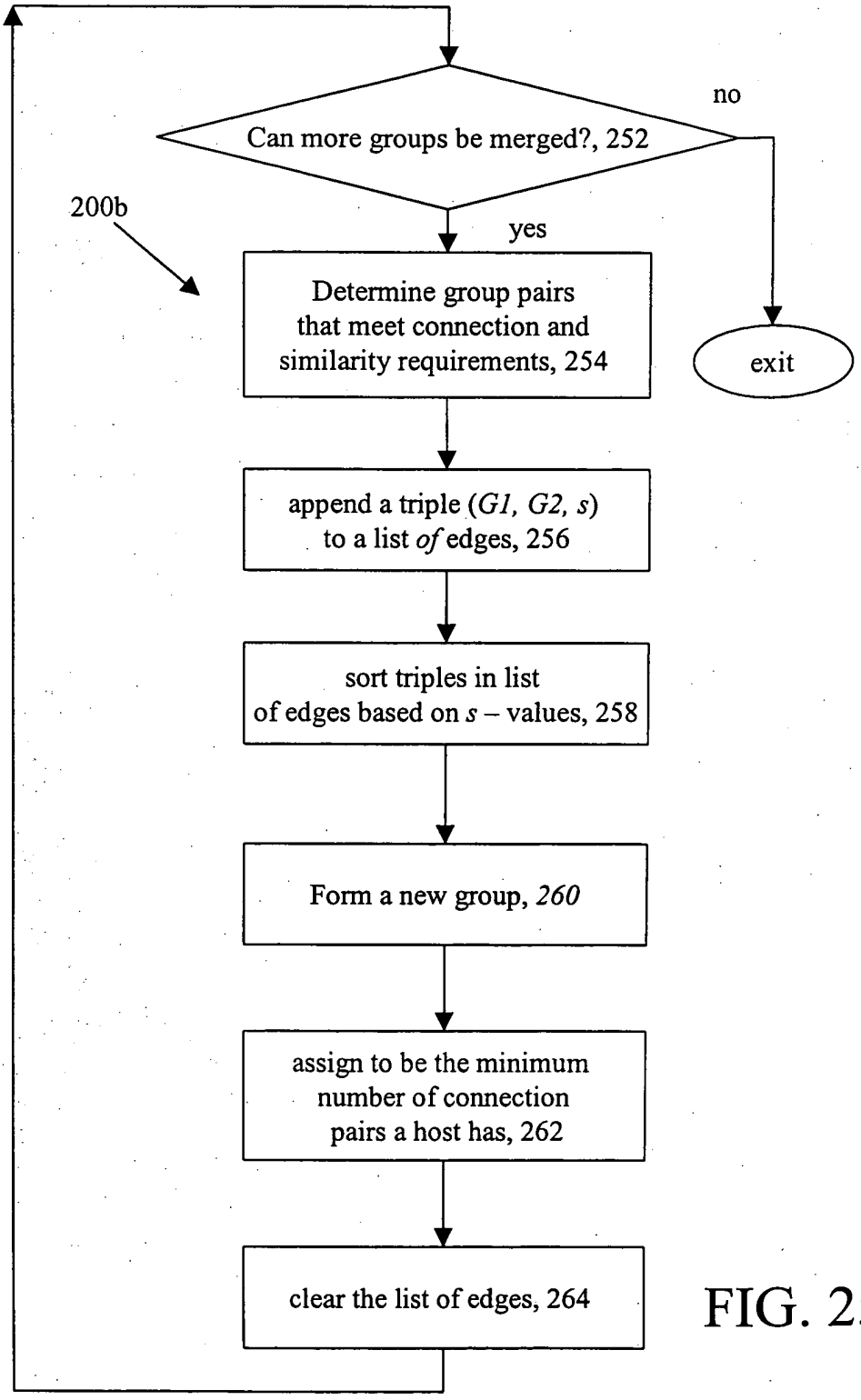

Can more groups be merged?, 252
no
yes
200b
Determine group pairs that meet connection and similarity requirements, 254
exit
append a triple (G1, G2, s) to a list of edges, 256
sort triples in list of edges based on s – values, 258
Form a new group, 260
assign to be the minimum number of connection pairs a host has, 262
clear the list of edges, 264

FIG. 25

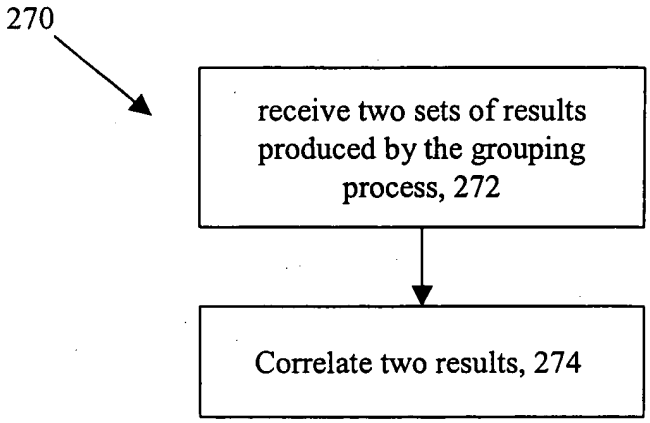

270
receive two sets of results produced by the grouping process, 272
Correlate two results, 274

FIG. 26

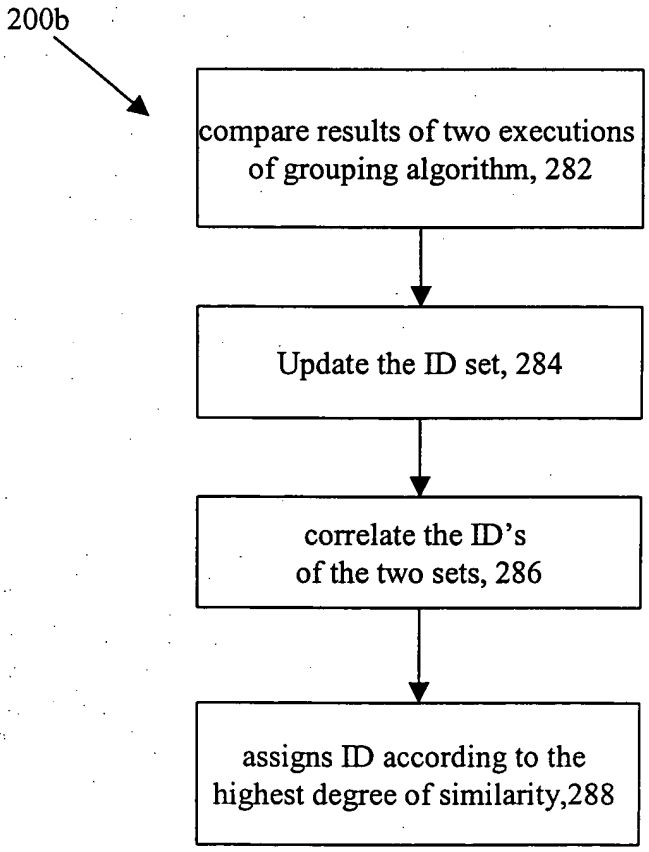

200b
compare results of two executions of grouping algorithm, 282
Update the ID set, 284
correlate the ID's of the two sets, 286
assigns ID according to the highest degree of similarity,288

FIG. 27

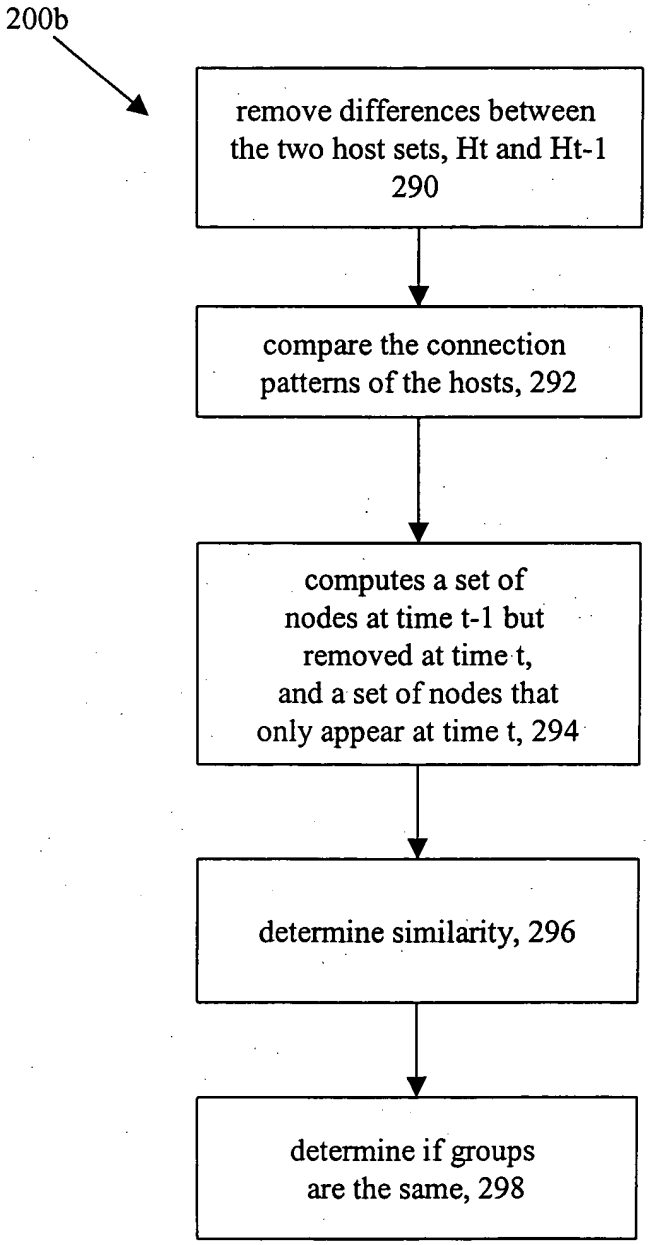

200b
remove differences between the two host sets, Ht and Ht-1 290
compare the connection patterns of the hosts, 292
computes a set of nodes at time t-1 but removed at time t, and a set of nodes that only appear at time t, 294
determine similarity, 296
determine if groups are the same, 298

FIG. 28

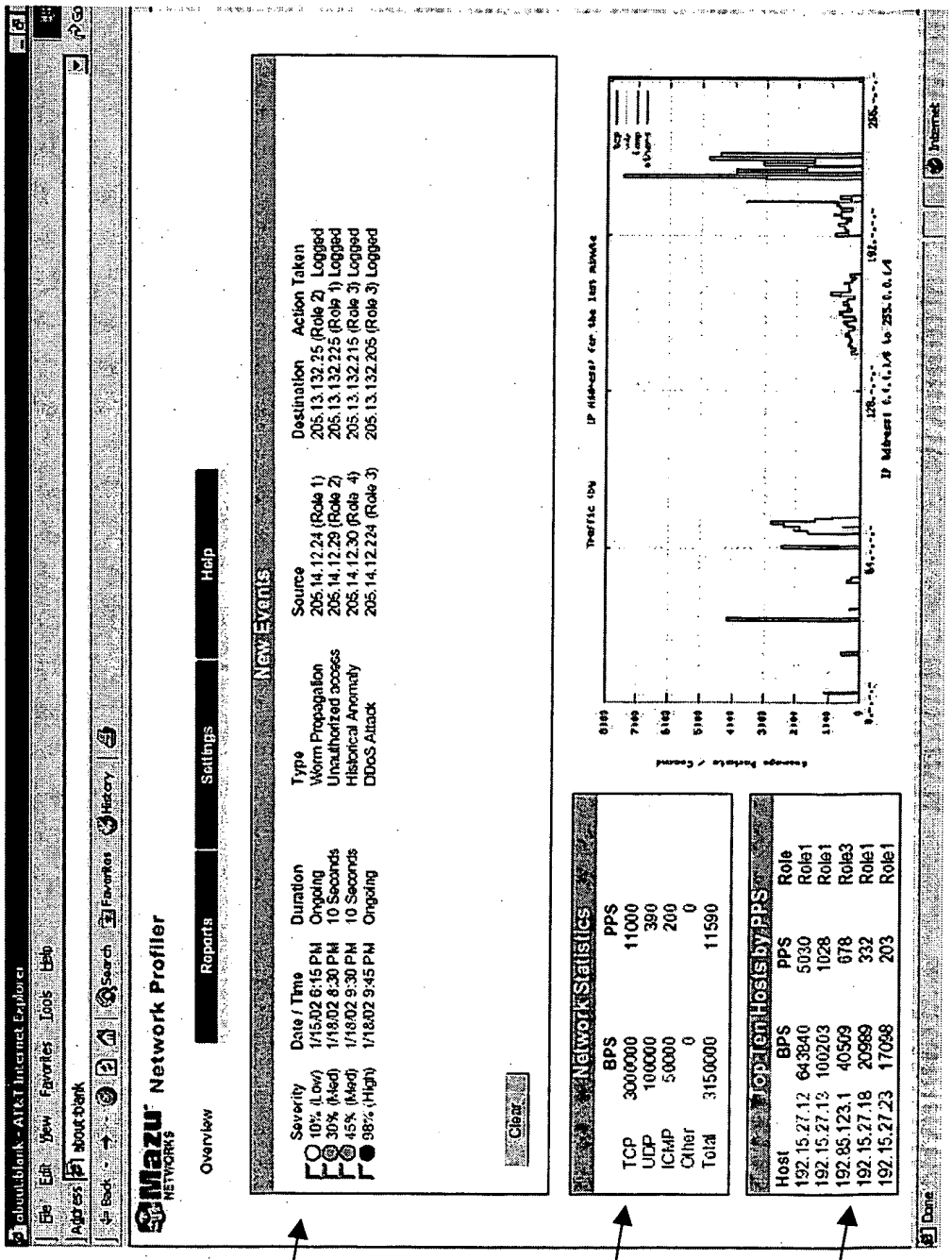

300
304
306
308
Network Profiler
Overview
Reports
Settings
Help
New Events
Severity
Date / Time
Duration
Type
Source
Destination
Action Taken
10% (Low) 1/15/02 6:15 PM Ongoing Worm Propagation 205.14.12.24 (Role 1) 205.13.132.25 (Role 2) Logged
30% (Med) 1/18/02 8:30 PM 10 Seconds Unauthorized access 205.14.12.29 (Role 2) 205.13.132.225 (Role 1) Logged
45% (Med) 1/18/02 9:30 PM 10 Seconds Historical Anomaly 205.14.12.30 (Role 4) 205.13.132.215 (Role 3) Logged
98% (High) 1/18/02 9:45 PM Ongoing DDoS Attack 205.14.12.224 (Role 3) 205.13.132.205 (Role 3) Logged
Clear
Network Statistics
BPS
PPS
TCP 3000000 11000
UDP 100000 390
ICMP 50000 200
Other 0 0
Total 3150000 11590
Top Ten Hosts by PPS
Host
BPS
PPS
Role
192.15.27.12 643840 5030 Role1
192.15.27.13 100203 1028 Role1
192.85.123.1 40509 678 Role3
192.15.27.18 20989 332 Role1
192.15.27.23 17098 203 Role1

FIG. 29

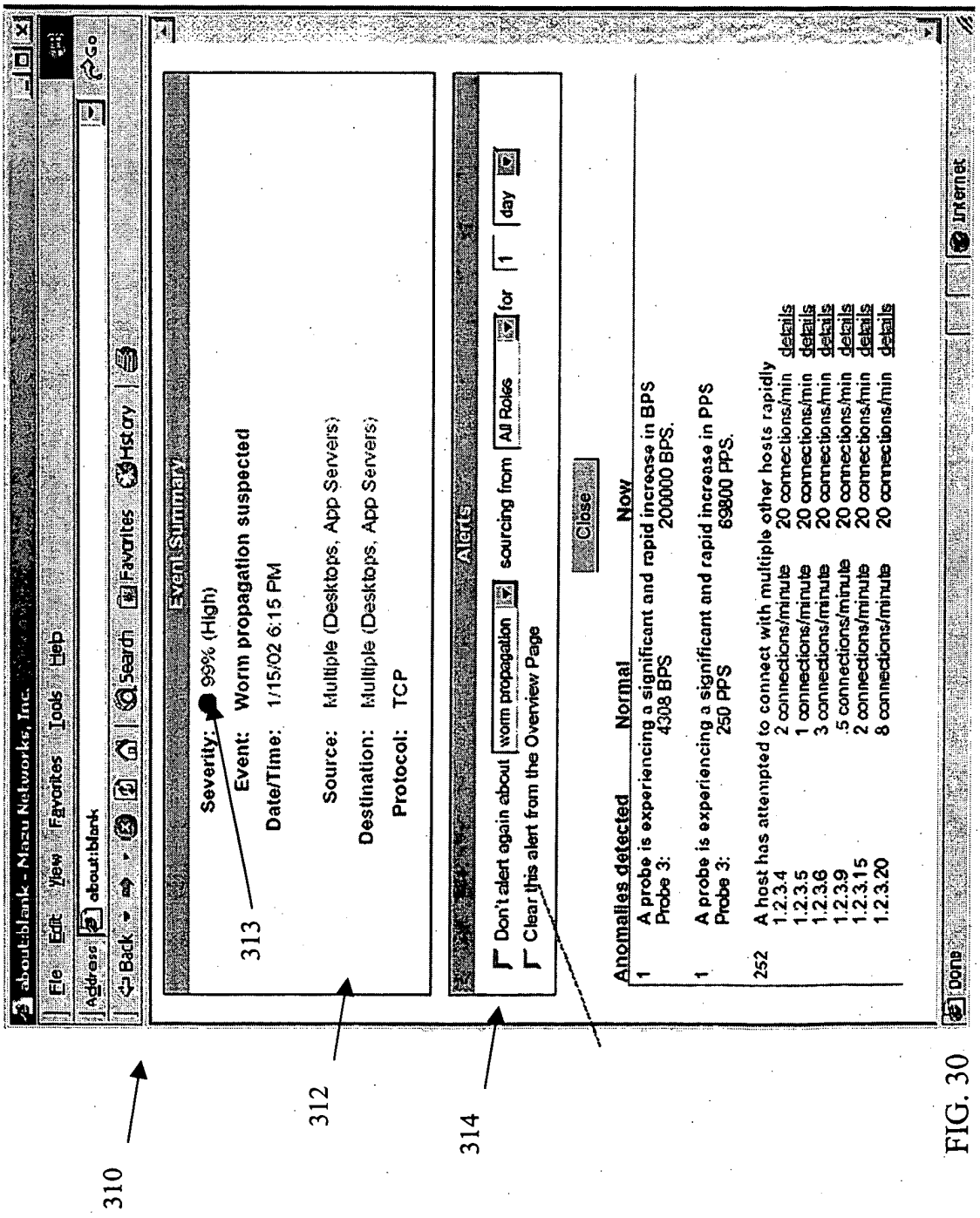

310
312
313
314
about:blank - Mazu Networks, Inc.
File Edit View Favorites Tools Help
Address about:blank
Back Search Favorites History
Event Summary
Severity: 99% (High)
Event: Worm propagation suspected
Date/Time: 1/15/02 6:15 PM
Source: Multiple (Desktops, App Servers)
Destination: Multiple (Desktops, App Servers)
Protocol: TCP
Alerts
Don't alert again about worm propagation sourcing from All Roles for 1 day
Clear this alert from the Overview Page
Close
Anomalies detected Normal Now
1 A probe is experiencing a significant and rapid increase in BPS
Probe 3: 4308 BPS 200000 BPS.
1 A probe is experiencing a significant and rapid increase in PPS
Probe 3: 250 PPS 69800 PPS.
252 A host has attempted to connect with multiple other hosts rapidly
1.2.3.4 2 connections/minute 20 connections/min details
1.2.3.5 1 connections/minute 20 connections/min details
1.2.3.6 3 connections/minute 20 connections/min details
1.2.3.9 .5 connections/minute 20 connections/min details
1.2.3.15 2 connections/minute 20 connections/min details
1.2.3.20 8 connections/minute 20 connections/min details
Done
Internet

FIG. 30

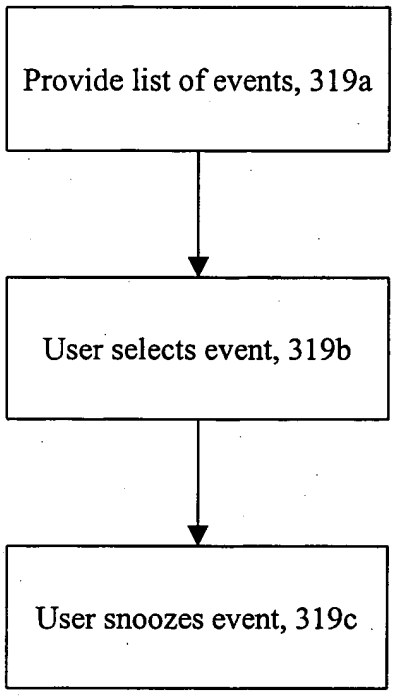

Provide list of events, 319a
User selects event, 319b
User snoozes event, 319c

FIG. 31

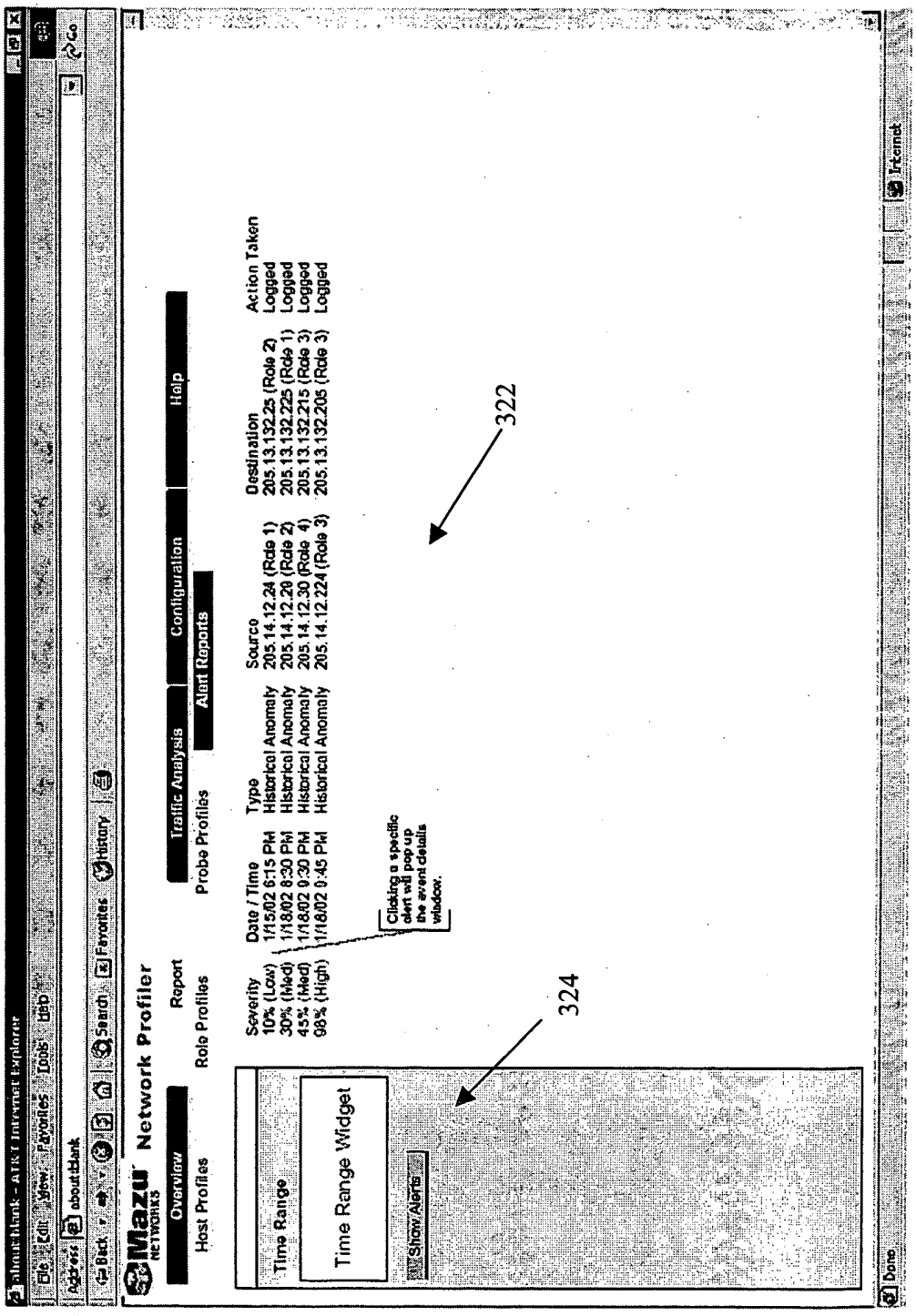

about:blank - AT&T Internet Explorer
File Edit View Favorites Tools Help
Address about:blank
Back Search Favorites History
Done
Internet
Mazu NETWORKS
Network Profiler
Overview
Report
Traffic Analysis
Configuration
Help
Host Profiles
Role Profiles
Probe Profiles
Alert Reports
Time Range
Time Range Widget
Show Alerts
Severity
Date / Time
Type
Source
Destination
Action Taken
10% (Low) 1/15/02 6:15 PM Historical Anomaly 205.14.12.24 (Role 1) 205.13.132.25 (Role 2) Logged
30% (Med) 1/18/02 8:30 PM Historical Anomaly 205.14.12.28 (Role 2) 205.13.132.225 (Role 1) Logged
45% (Med) 1/18/02 9:30 PM Historical Anomaly 205.14.12.30 (Role 4) 205.13.132.215 (Role 3) Logged
98% (High) 1/18/02 9:45 PM Historical Anomaly 205.14.12.224 (Role 3) 205.13.132.205 (Role 3) Logged
Clicking a specific alert will pop up the event details window.
322
324

FIG. 32

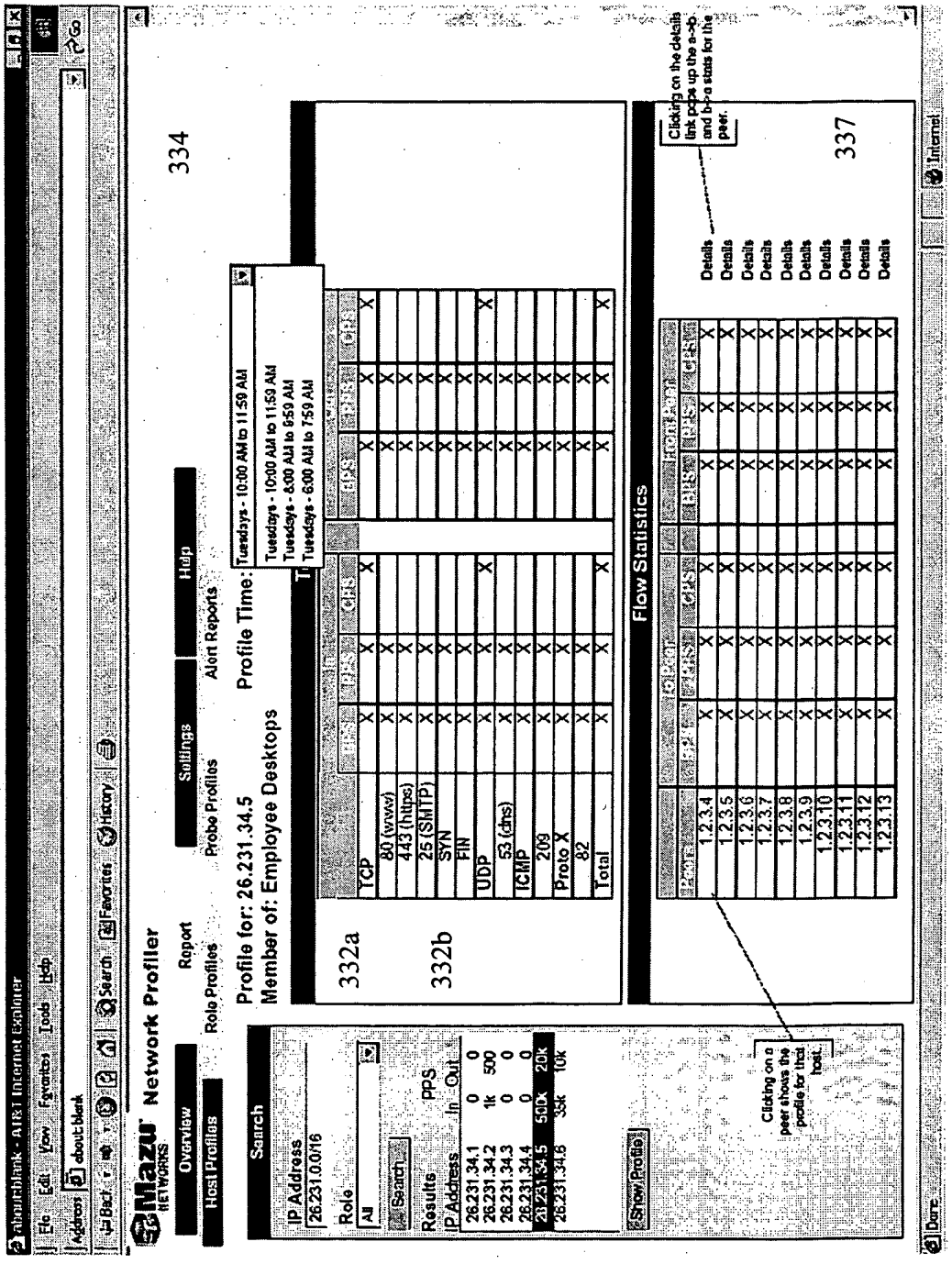

Network Profiler
Overview
Report
Settings
Help
Host Profiles
Role Profiles
Probe Profiles
Alert Reports
Search
IP Address
26.231.0.0/16
Role
All
Search
Results
IP Address
PPS
In
Out
26.231.34.1
26.231.34.2
26.231.34.3
26.231.34.4
26.231.34.5
26.231.34.8
Show Profile
Clicking on a peer shows the profile for that host.
Profile for: 26.231.34.5
Member of: Employee Desktops
Profile Time:
Tuesdays - 10:00 AM to 11:59 AM
Tuesdays - 8:00 AM to 9:59 AM
Tuesdays - 6:00 AM to 7:59 AM
TCP
80 (www)
443 (https)
25 (SMTP)
SYN
FIN
UDP
53 (dns)
ICMP
209
Proto X
82
Total
Flow Statistics
1.2.3.4
1.2.3.5
1.2.3.6
1.2.3.7
1.2.3.8
1.2.3.9
1.2.3.10
1.2.3.11
1.2.3.12
1.2.3.13
Details
Clicking on the details link pops up the a->b and b->a stats for the peer.
Done
Internet
334
332
332a
332b
330
336
337

FIG. 33

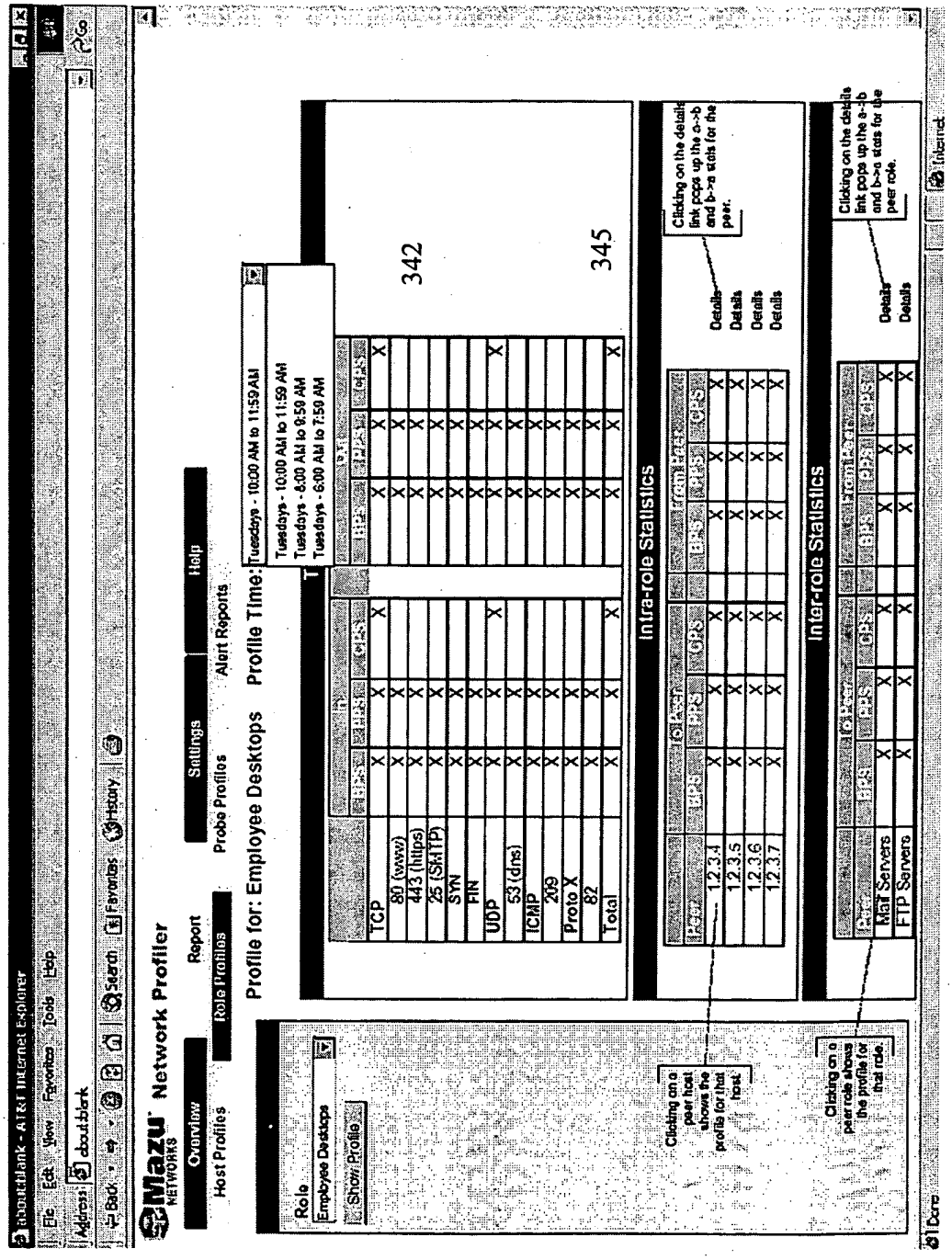

Network Profiler
Overview
Report
Settings
Help
Host Profiles
Role Profiles
Probe Profiles
Alert Reports
Profile for: Employee Desktops
Profile Time:
Tuesdays - 10:00 AM to 11:59 AM
Tuesdays - 8:00 AM to 9:59 AM
Tuesdays - 6:00 AM to 7:59 AM
Role
Employee Desktops
Show Profile
TCP
80 (www)
443 (https)
25 (SMTP)
SYN
FIN
UDP
53 (dns)
ICMP
209
Proto X
82
Total
342
345
Intra-role Statistics
Inter-role Statistics
Clicking on a peer host shows the profile for that host.
Clicking on a peer role shows the profile for that role.
Clicking on the details link pops up the a->b and b->a stats for the peer.
Details
1.2.3.4
1.2.3.5
1.2.3.6
1.2.3.7
Mail Servers
FTP Servers
341
340
346
347
344

FIG. 34

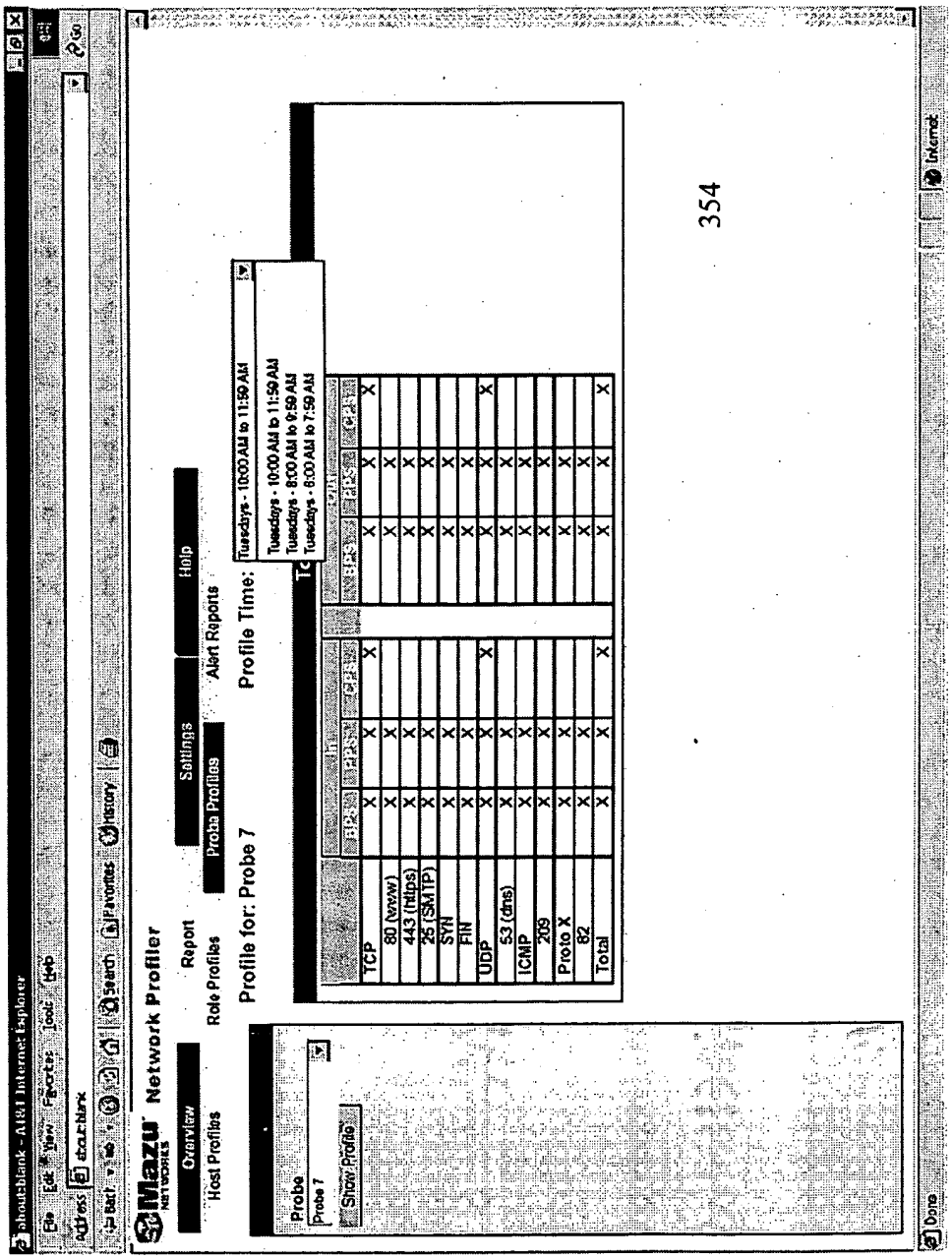

about:blank - Alert Internet Explorer
Network Profiler
Overview
Report
Settings
Help
Host Profiles
Role Profiles
Probe Profiles
Alert Reports
Probe
Probe 7
Show Profile
Profile for: Probe 7
Profile Time:
Tuesdays - 10:00 AM to 11:59 AM
Tuesdays - 10:00 AM to 11:59 AM
Tuesdays - 8:00 AM to 9:59 AM
Tuesdays - 8:00 AM to 7:59 AM
TCP
80 (www)
443 (https)
25 (SMTP)
SYN
FIN
UDP
53 (dns)
ICMP
209
Proto X
82
Total
Done
Internet
352
354

FIG. 35

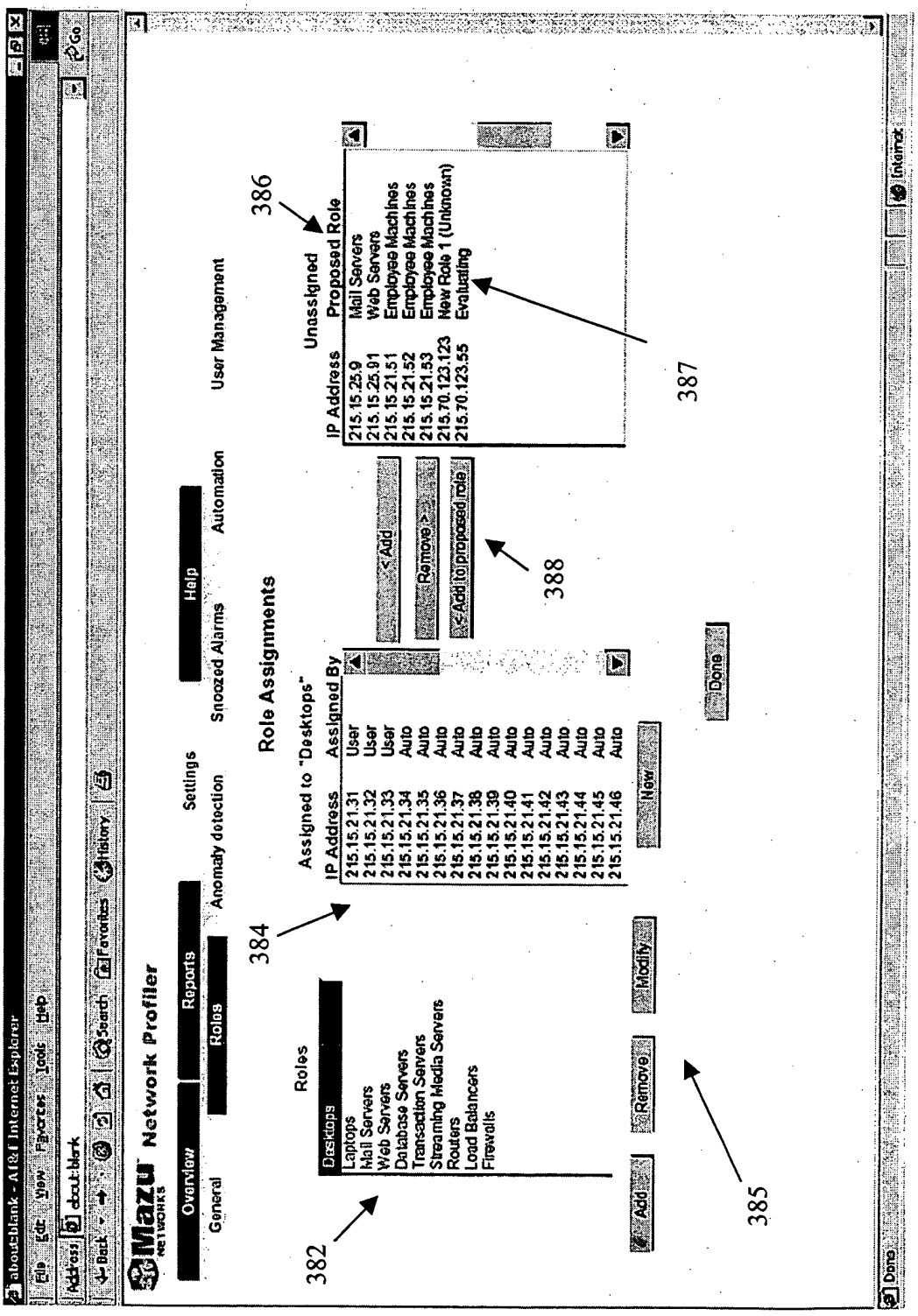
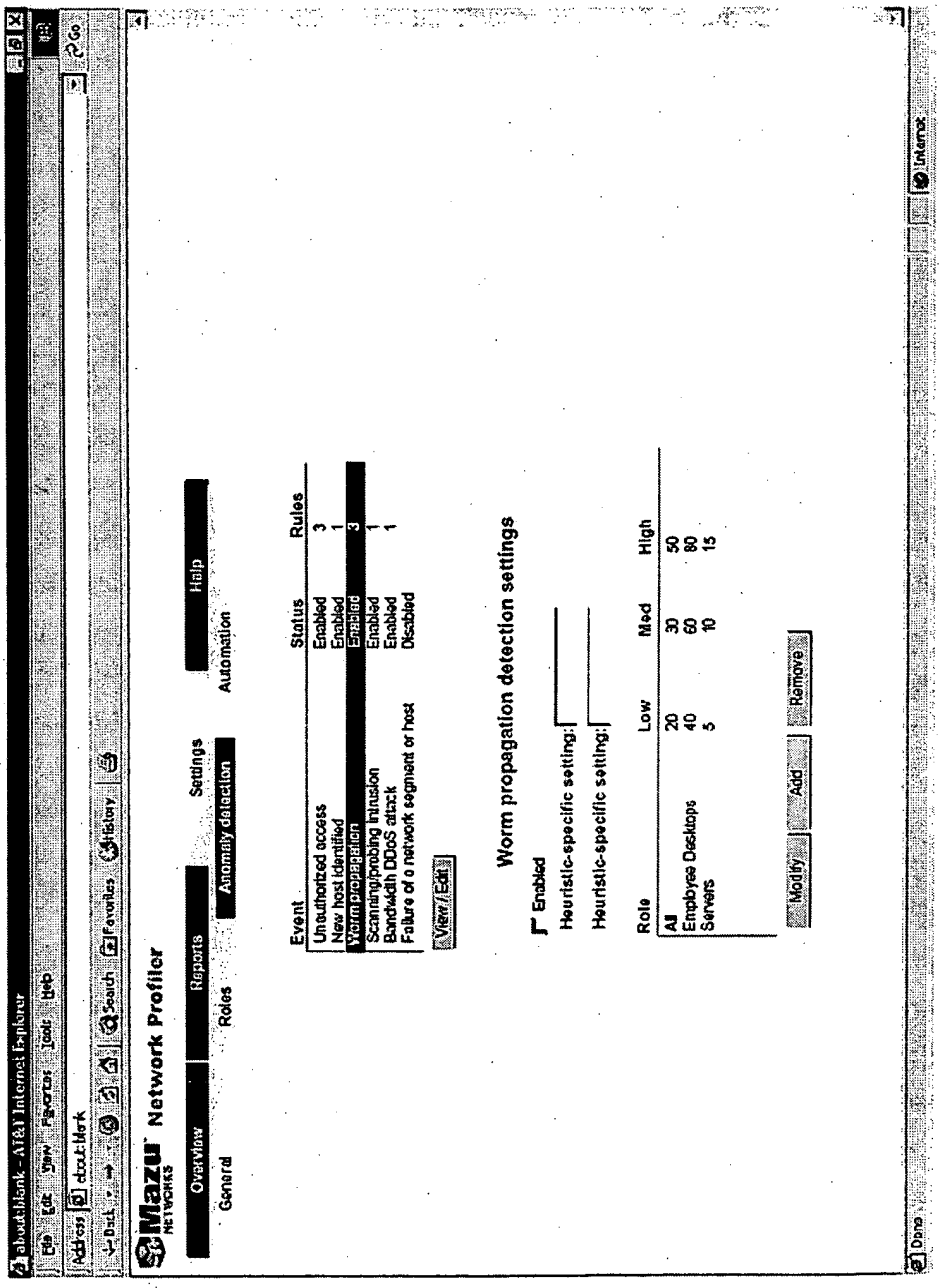
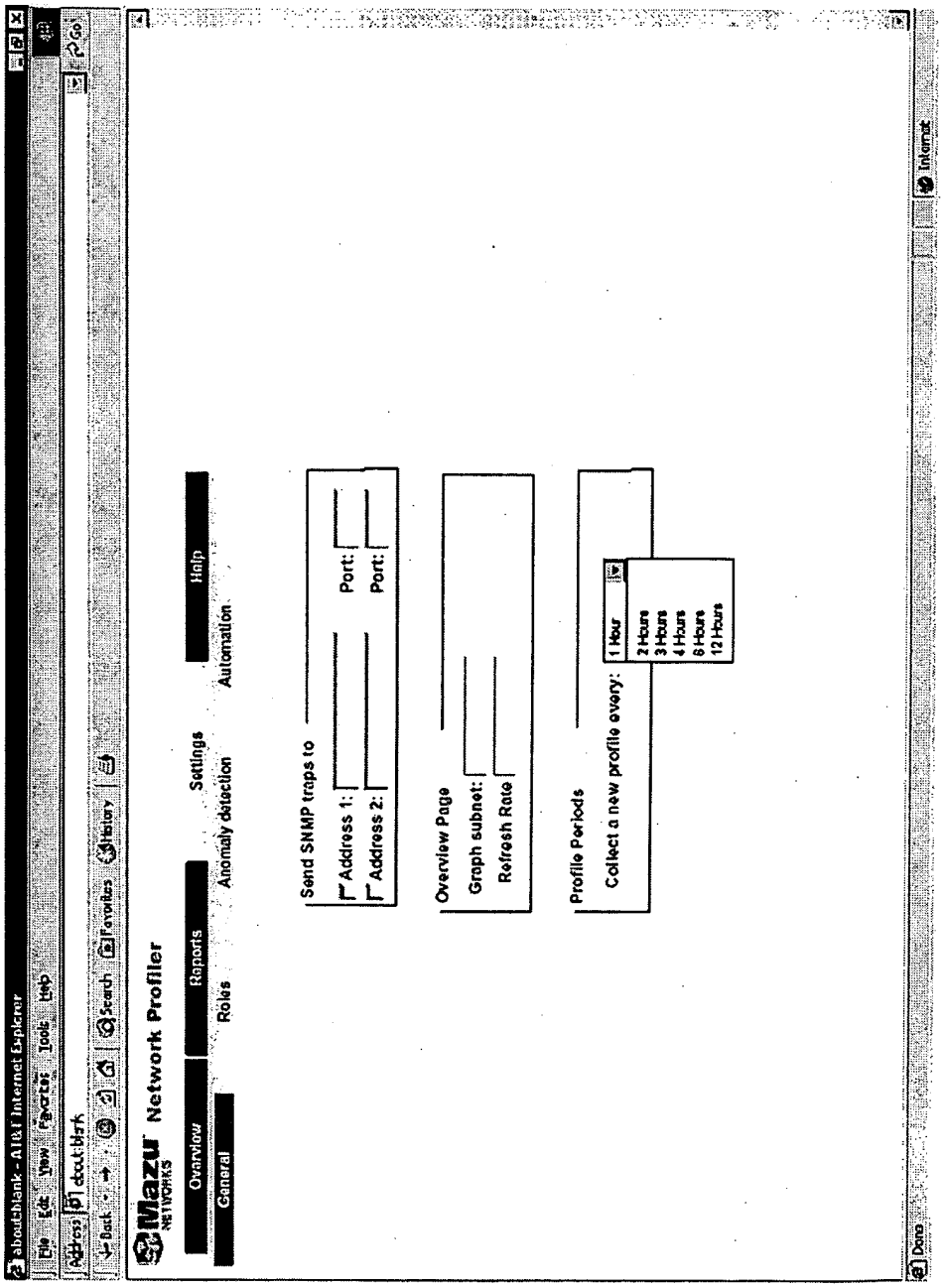

aboutblank - AT&T Internet Explorer
Mazu Network Profiler
Overview
Reports
Settings
Help
General
Roles
Anomaly detection
Snoozed Alarms
Automation
User Management
Roles
Desktops
Laptops
Mail Servers
Web Servers
Database Servers
Transaction Servers
Streaming Media Servers
Routers
Load Balancers
Firewalls
Role Assignments
Assigned to "Desktops"
IP Address
Assigned By
215.15.21.31 User
215.15.21.32 User
215.15.21.33 User
215.15.21.34 Auto
215.15.21.35 Auto
215.15.21.36 Auto
215.15.21.37 Auto
215.15.21.38 Auto
215.15.21.39 Auto
215.15.21.40 Auto
215.15.21.41 Auto
215.15.21.42 Auto
215.15.21.43 Auto
215.15.21.44 Auto
215.15.21.45 Auto
215.15.21.46 Auto
<Add
Remove >>
<< Add to proposed role
Unassigned
IP Address
Proposed Role
215.15.25.9 Mail Servers
215.15.25.91 Web Servers
215.15.21.51 Employee Machines
215.15.21.52 Employee Machines
215.15.21.53 Employee Machines
215.70.123.123 New Role 1 (Unknown)
215.70.123.55 Evaluating
Add
Remove
Modify
New
Done
382
384
385
386
387
388
380

FIG. 36


about:blank - AT&T Internet Explorer
File Edit View Favorites Tools Help
Address about:blank
Back Search Favorites History
Done
Internet
Mazu Networks
Network Profiler
Overview
Reports
Settings
Help
General
Roles
Anomaly detection
Automation
Event
Status
Rules
Unauthorized access
Enabled
3
New host identified
Enabled
1
Worm propagation
Enabled
3
Scanning/probing intrusion
Enabled
1
Bandwidth DDoS attack
Enabled
1
Failure of a network segment or host
Disabled
1
View / Edit
Worm propagation detection settings
Enabled
Heuristic-specific setting:
Heuristic-specific setting:
Role
Low
Med
High
All
20
30
50
Employee Desktops
40
60
80
Servers
5
10
15
Modify
Add
Remove

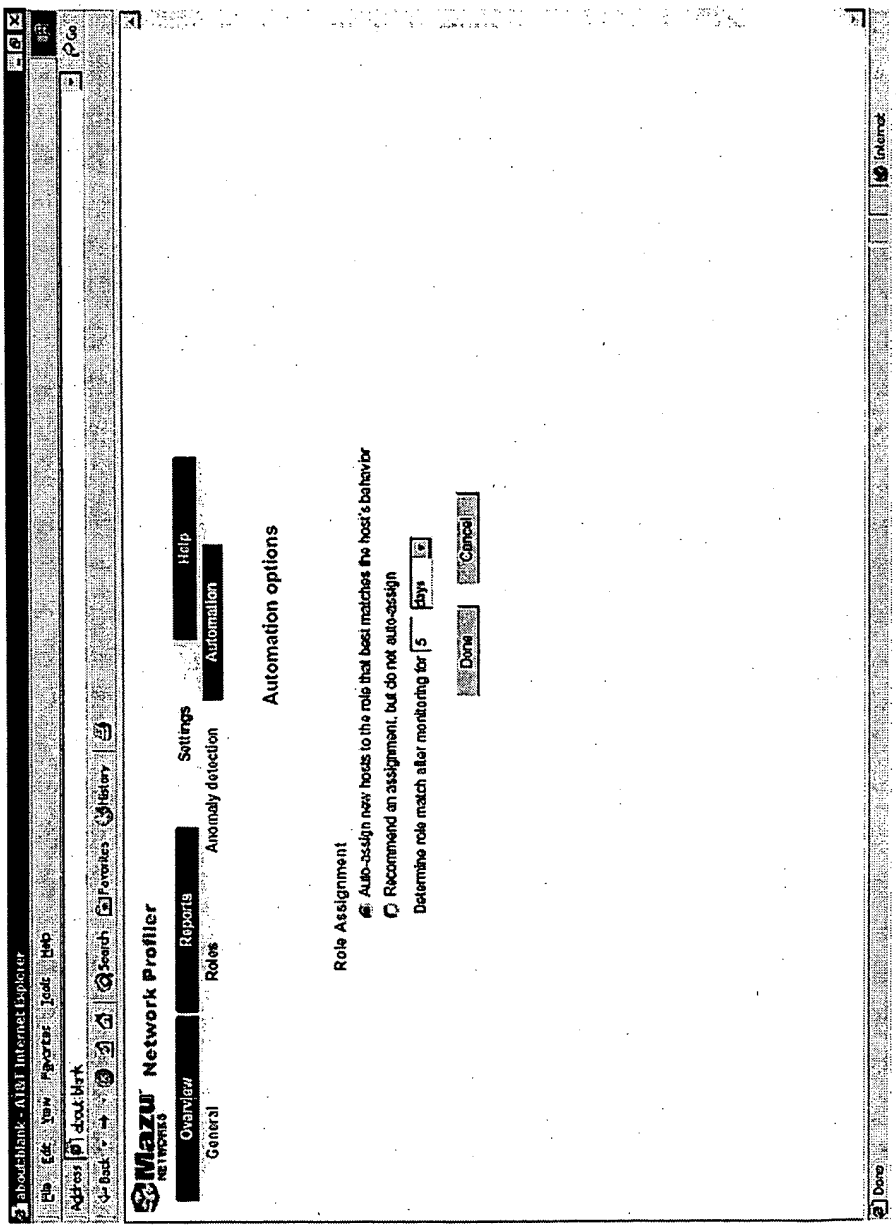
400

FIG. 37


about:blank - AT&T Internet Explorer
File Edit View Favorites Tools Help
Address about:blank
Back Search Favorites History
Mazu NETWORKS
Network Profiler
Overview
Reports
Settings
Help
General
Roles
Anomaly detection
Automation
Send SNMP traps to
Address 1:
Port:
Address 2:
Port:
Overview Page
Graph subnet:
Refresh Rate
Profile Periods
Collect a new profile every:
1 Hour
2 Hours
3 Hours
4 Hours
8 Hours
12 Hours
Done
Internet

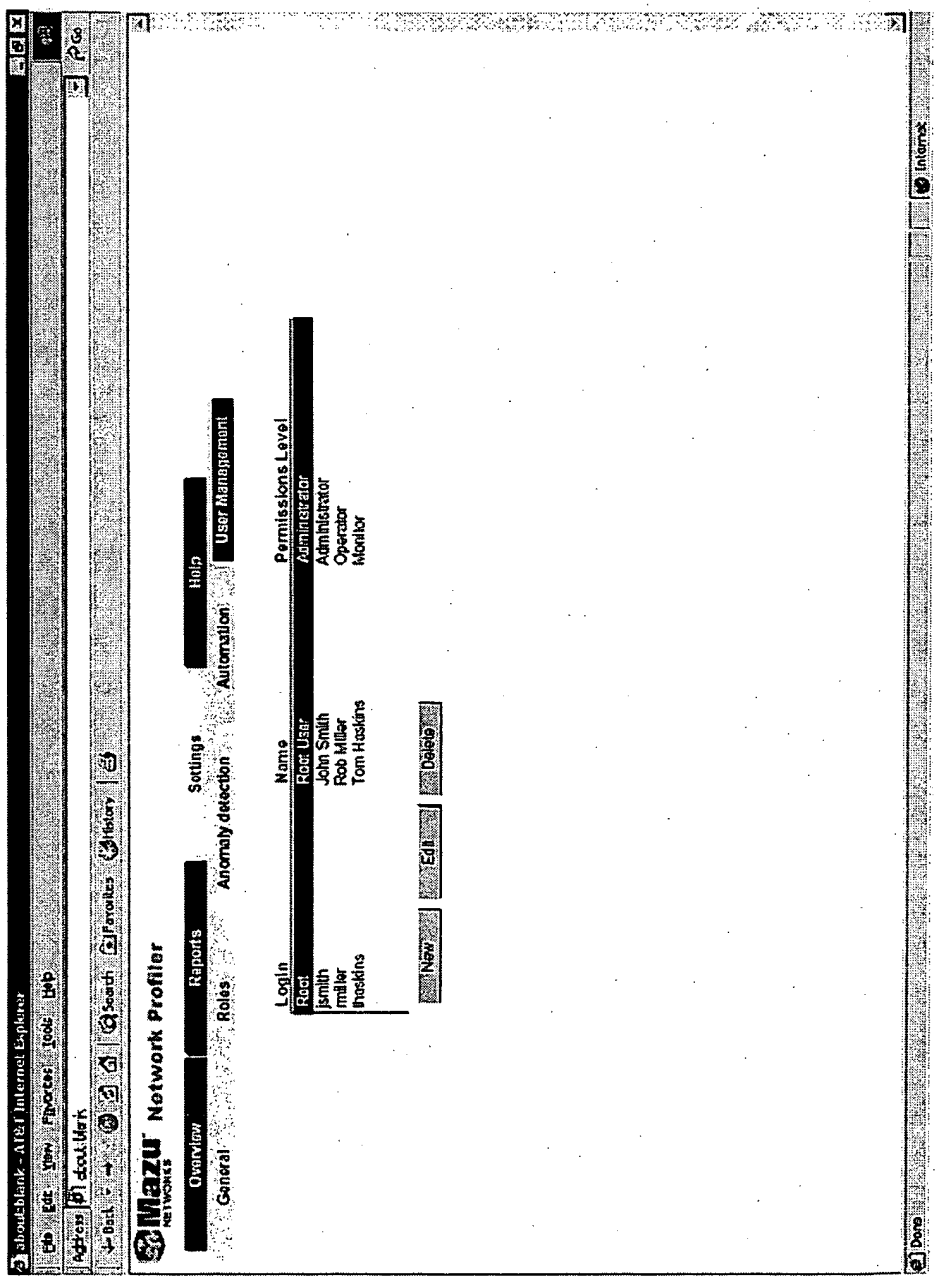
410

FIG. 38


about:blank - AT&T Internet Explorer
File Edit View Favorites Tools Help
Address about:blank
Back Search Favorites History
Mazu Networks
Network Profiler
Overview
Reports
Settings
Help
General
Roles
Anomaly detection
Automation
Automation options
Role Assignment
Auto-assign new hosts to the role that best matches the host's behavior
Recommend an assignment, but do not auto-assign
Determine role match after monitoring for 5 days
Done
Cancel
Done
Internet

420

FIG. 39


about:blank - AT&T Internet Explorer
File Edit View Favorites Tools Help
Address about:blank
Back Search Favorites History
Mazu Networks
Network Profiler
Overview
Reports
Settings
Help
General
Roles
Anomaly detection
Automation
User Management
Login
Name
Permissions Level
Root
Root User
Administrator
jsmith
John Smith
Administrator
rmiller
Rob Miller
Operator
thoskins
Tom Hoskins
Monitor
New
Edit
Delete
Done
Internet

430

FIG. 40